Novell Identity Manager

3.0

www.novell.com

8 de dezembro de 2005

APLICATIVO DE USUÁRIO DO IDENTITY MANAGER: GUIA DE ADMINISTRAÇÃO

Novell®

Informações legais

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
EUA
www.novell.com

Documentação Online: Para acessar a documentação online deste e de outros produtos da Novell e obter atualizações, consulte www.novell.com/documentation.

Marcas registradas da Novell

Materiais de terceiros

Todas as marcas registradas de terceiros pertencem aos seus respectivos proprietários.

Informações legais de terceiros

Licença do The Apache Software, Versão 1.1

Copyright (c) 2000 The Apache Software Foundation. Todos os direitos reservados.

A redistribuição e o uso nos formatos de código-fonte e binário, com ou sem modificações, são permitidos contanto que as condições a seguir sejam atendidas:

1. A redistribuição do código-fonte deve apresentar o aviso de copyright acima, esta lista de condições e a seguinte isenção de responsabilidade.
2. A redistribuição em formato binário deve reproduzir o aviso de copyright acima, esta lista de condições e a seguinte isenção de responsabilidade na documentação e/ou qualquer material fornecido na distribuição.
3. A documentação do usuário final incluída com a redistribuição, se existente, deve incluir o seguinte aviso: "Este produto inclui o software desenvolvido pela Apache Software Foundation (http://www.apache.org/)."

Como alternativa, esse aviso poderá ser exibido no próprio software se, e sempre que, tais avisos de terceiros forem normalmente exibidos.

4. Os nomes "Apache" e "Apache Software Foundation" não devem ser usados para recomendar ou promover produtos derivados deste software sem permissão prévia por escrito. Para obter permissão por escrito, entre em contato com apache@apache.org.
5. Os produtos derivados deste software não podem ser denominados "Apache", e a palavra "Apache" não deve fazer parte de seu nome sem a permissão prévia por escrito da Apache Software Foundation.

ESTE SOFTWARE É FORNECIDO "NO ESTADO EM QUE SE ENCONTRA" E NÃO OFERECE NENHUMA GARANTIA, EXPRESSA OU IMPLÍCITA, INCLUINDO, MAS NÃO SE LIMITANDO A, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO OU ADEQUAÇÃO A UM PROPÓSITO ESPECÍFICO. SOB NENHUMA CIRCUNSTÂNCIA A APACHE SOFTWARE FOUNDATION OU SEUS COLABORADORES SERÃO RESPONSÁVEIS POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQÜENCIAL (INCLUINDO, MAS NÃO SE LIMITANDO A, COMPRA DE BENS OU SERVIÇOS SUBSTITUTOS; PERDA DA CAPACIDADE DE USO, DADOS OU LUCRO; OU INTERRUPÇÃO DAS OPERAÇÕES COMERCIAIS) QUALQUER QUE SEJA SUA CAUSA E DE ACORDO COM QUALQUER TEORIA DE RESPONSABILIDADE, ESTEJA OU NÃO PREVISTA EM CONTRATO, RESPONSABILIDADE ESTRITA OU DELITO (INCLUINDO OU NÃO NEGLIGÊNCIA), CAUSADOS PELO USO DESTE SOFTWARE, MESMO QUE ESTEJAM CIENTES DA POSSIBILIDADE DO DANO.

Autonomy

Copyright ©1996-2000 Autonomy, Inc.

Bouncy Castle

License Copyright (c) 2000 - 2004 The Legion Of The Bouncy Castle (http://www.bouncycastle.org)

A permissão é concedida por meio deste, gratuitamente, a qualquer pessoa que obtenha uma cópia deste software e arquivos de documentação associados (o "Software") para utilizar o Software sem restrições, incluindo, mas não se limitando a, direitos ao uso, cópia, modificação, mesclagem, publicação, distribuição, sub-licenciamento e/ou venda de cópias do Software, e de conceder os mesmos direitos a outras pessoas às quais o Software for distribuído, de acordo com as seguintes condições:

O aviso de copyright acima e este aviso de permissão devem ser incluídos em todas as cópias ou partes substanciais do Software.

ESTE SOFTWARE É FORNECIDO "NO ESTADO EM QUE SE ENCONTRA" E NÃO OFERECE NENHUMA GARANTIA, EXPRESSA OU IMPLÍCITA, INCLUINDO, MAS NÃO SE LIMITANDO A, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO OU ADEQUAÇÃO A UM PROPÓSITO ESPECÍFICO E NÃO-INFRAÇÃO. SOB NENHUMA CIRCUNSTÂNCIA OS AUTORES OU PROPRIETÁRIOS DE DIREITOS AUTORAIS SERÃO RESPONSÁVEIS POR QUALQUER AÇÃO, DANOS OU OUTRAS RESPONSABILIDADES, PREVISTAS OU NÃO EM CONTRATO, EM DELITO, CAUSADAS PELO OU EM

CONEXÃO AO SOFTWARE OU O USO OU OUTRA APLICAÇÃO DO SOFTWARE.

Castor Library

A licença original pode ser encontrada em http://www.castor.org/license.html

O código-fonte desse projeto foi lançado de acordo com uma licença [license.txt] do tipo BSD:

A redistribuição e o uso deste software e sua documentação associada ("Software"), com ou sem modificações, são permitidos contanto que as condições a seguir sejam atendidas:

1. A redistribuição do código-fonte deve apresentar avisos e declarações de copyright. As redistribuições devem conter também uma cópia deste documento.
2. A redistribuição em formato binário deve reproduzir o aviso de copyright acima, esta lista de condições e a isenção de responsabilidade a seguir na documentação e/ou qualquer material fornecido na distribuição.
3. O nome "ExoLab" não deve ser usado para recomendar ou promover produtos derivados deste Software sem permissão prévia por escrito da Intalio Inc. Para solicitar a permissão por escrito, entre em contato com info@exolab.org.
4. Os produtos derivados deste Software não podem ser denominados "Castor", e a palavra "Castor" não deve fazer parte de seu nome sem a permissão prévia por escrito da Intalio Inc. Exolab. Castor e Intalio são marcas registradas da Intalio Inc.
5. O crédito apropriado deve ser dado ao ExoLab Project (http://www.exolab.org/).

ESTE SOFTWARE É FORNECIDO PELA INTALIO E SEUS COLABORADORES "NO ESTADO EM QUE SE ENCONTRA" E NÃO OFERECE NENHUMA GARANTIA, EXPRESSA OU IMPLÍCITA, INCLUINDO, MAS NÃO SE LIMITANDO A, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO OU ADEQUAÇÃO A UM PROPÓSITO ESPECÍFICO. SOB NENHUMA CIRCUNSTÂNCIA A INTALIO OU SEUS COLABORADORES SERÃO RESPONSÁVEIS POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQÜENCIAL (INCLUINDO, MAS NÃO SE LIMITANDO A, COMPRA DE BENS OU SERVIÇOS SUBSTITUTOS; PERDA DA CAPACIDADE DE USO, DADOS OU LUCRO; OU INTERRUPÇÃO DAS OPERAÇÕES COMERCIAIS), QUALQUER QUE SEJA SUA CAUSA E DE ACORDO COM QUALQUER TEORIA DE RESPONSABILIDADE, SEJA EM CONTRATO, RESPONSABILIDADE ESTRITA OU DELITO (INCLUINDO OU NÃO NEGLIGÊNCIA), CAUSADOS PELO USO DESTE SOFTWARE, MESMO QUE ESTEJAM CIENTES DA POSSIBILIDADE DO DANO.

Licença de Software do Indiana University Extreme! Lab

Versão 1.1.1

A redistribuição e o uso nos formatos de código-fonte e binário, com ou sem modificações, são permitidos contanto que as condições a seguir sejam atendidas:

1. A redistribuição do código-fonte deve apresentar o aviso de copyright acima, esta lista de condições e a seguinte isenção de responsabilidade.
2. A redistribuição em formato binário deve reproduzir o aviso de copyright acima, esta lista de condições e a seguinte isenção de responsabilidade na documentação e/ou qualquer material fornecido na distribuição.
3. A documentação do usuário final incluída com a redistribuição, se existente, deve incluir o seguinte aviso: "Este produto inclui o software desenvolvido pelo Indiana University Extreme! Lab (http://www.extreme.indiana.edu/)."

Como alternativa, esse aviso pode ser exibido no próprio software se, e sempre que, tais avisos de terceiros forem normalmente exibidos.

4. Os nomes "Indiana University" e "Indiana University Extreme! Lab" não devem ser usados para recomendar ou promover produtos derivados deste software sem permissão prévia por escrito. Para obter permissão por escrito, entre em contato com http://www.extreme.indiana.edu/.
5. Os produtos derivados deste software não podem usar o nome "Indiana University", e a palavra Indiana University" não deve fazer parte de seu nome sem permissão prévia por escrito da Indiana University.

ESTE SOFTWARE É FORNECIDO "NO ESTADO EM QUE SE ENCONTRA" E NÃO OFERECE NENHUMA GARANTIA, EXPRESSA OU IMPLÍCITA, INCLUINDO, MAS NÃO SE LIMITANDO A, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO OU ADEQUAÇÃO A UM PROPÓSITO ESPECÍFICO. SOB

existentes. Caso nenhum exista, o Aviso Curto do Software W3C (W3C Software Short Notice) deverá ser incluído (hipertexto é preferencial; texto é permitido) no corpo de qualquer código-fonte redistribuído ou derivado.

3. Aviso de quaisquer modificações aos arquivos, incluindo a data de tais modificações. (Recomendamos que você forneça os URIs do local de origem do código.)

ESTE SOFTWARE E DOCUMENTAÇÃO SÃO FORNECIDOS “NO ESTADO EM QUE SE ENCONTRAM”, E OS DETENTORES DOS DIREITOS AUTORAIS NÃO FAZEM REPRESENTAÇÕES NEM FORNECEM GARANTIAS, EXPRESSAS OU IMPLÍCITAS, INCLUINDO, MAS NÃO SE LIMITANDO A, GARANTIAS DE COMERCIALIZAÇÃO OU ADEQUAÇÃO A QUALQUER PROPÓSITO ESPECÍFICO, OU QUE O USO DO SOFTWARE OU DOCUMENTAÇÃO NÃO INFRINGE PATENTES, DIREITOS AUTORAIS, MARCAS COMERCIAIS OU OUTROS DIREITOS DE TERCEIROS.

OS DETENTORES DOS DIREITOS AUTORAIS NÃO PODEM SER RESPONSABILIZADOS POR QUAISQUER DANOS DIRETOS, INDIRETOS, ESPECIAIS OU CONSEQÜENCIAIS QUE RESULTEM DE QUALQUER USO DO SOFTWARE OU DOCUMENTAÇÃO.

O nome e marcas registradas dos detentores dos direitos autorais NÃO podem ser usados em anúncios ou publicidade associada ao software sem a permissão específica prévia por escrito. Os direitos autorais sobre o software e qualquer documentação associada serão sempre dos detentores dos direitos autorais.

Índice

Sobre este manual

Finalidade

Este manual descreve como administrar o *aplicativo de usuário* do Novell Identity Manager, incluindo:

- Os recursos de *Auto-Atendimento de Identidade* fornecidos com o Identity Manager
- Os recursos de *aprovisionamento baseado em workflow* se você adicionar o Módulo de Aprovisionamento do Identity Manager

Para saber como administrar outros recursos do Identity Manager (comuns a todos os pacotes), consulte o *Novell Identity Manager: Guia de Administração*.

Público-alvo

As informações neste manual destinam-se a *consultores, arquitetos e administradores de sistema* responsáveis pela *configuração, distribuição e gerenciamento* dos recursos do auto-atendimento de identidade e/ou dos recursos de aprovisionamento baseado em workflow do aplicativo de usuário do Identity Manager.

A documentação do usuário final desses recursos é fornecida no *Aplicativo de Usuário do Identity Manager: Guia do Usuário*.

Pré-requisitos

Este manual presume que:

- *Você tenha instalado* o Identity Manager e, possivelmente, o Módulo de Aprovisionamento do Identity Manager.

Para obter instruções de instalação desses produtos, consulte o *Novell Identity Manager: Guia de Instalação*.

- *Você tenha configurado* os outros recursos do Identity Manager de acordo com suas necessidades

Consulte o *Novell Identity Manager: Guia de Administração*.

Organização

Este é um resumo do que você encontrará neste manual:

Parte	Descrição
Parte I, "Visão geral" na página 11	Apresenta o aplicativo de usuário do Identity Manager e o ajuda a planejar seu uso em sua organização

Parte	Descrição
Parte II, “Configurando o ambiente do aplicativo de usuário” na página 55	Como configurar os vários aspectos do ambiente do aplicativo de usuário do Identity Manager (incluindo o driver, a camada de abstração do diretório e o registro do aplicativo de usuário) para atender às necessidades de sua organização
Parte III, “Administrando o aplicativo de usuário” na página 129	Como configurar e gerenciar o aplicativo de usuário do Identity Manager usando a guia Administração da interface de usuário
Parte IV, “Referência de portlet” na página 235	Como configurar os portlets de identidade e sistema usados na interface de usuário do Identity Manager
Parte V, “Criando e gerenciando solicitações de aprovisionamento” na página 305	Como configurar, distribuir e gerenciar os recursos e workflows e solicitar as definições necessárias para o aprovisionamento usando o Módulo de Aprovisionamento do Identity Manager **Observação:** Essa parte será pertinente somente se você tiver o Módulo de Aprovisionamento do Identity Manager.
Parte VI, “Apêndices” na página 359	Informações de referência adicionais (extensões de esquema) e tópicos avançados (configuração do arquivo do aplicativo) do aplicativo de usuário do Identity Manager

Consulte também

Para obter manuais relacionados e informações de arquivo readme, vá para a página do Identity Manager (http://www.novell.com/idm/) no site de documentação da Novell na Web.

Visão geral

Estes capítulos apresentam o aplicativo de usuário do Identity Manager e o ajudam a planejar seu uso em sua organização.

1 Visão geral

O aplicativo de usuário do Novell Identity Manager é um aplicativo Web robusto projetado para proporcionar ao usuário uma experiência satisfatória, intuitiva, altamente configurável e fácil de administrar com uma sofisticada estrutura de serviços de identidade adjacente. Quando usado em conjunto com o Módulo de Aprovisionamento do Identity Manager e Novell Audit, o aplicativo de usuário do Identity Manager fornece uma solução de aprovisionamento completa e abrangente que é também segura, escalável e fácil de gerenciar.

O aplicativo de usuário oferece os seguintes recursos de usuário final baseados na Web:

- White pages
- Organogramas
- Pesquisa do usuário (com a capacidade de gravar configurações de pesquisas personalizadas)
- Gerenciamento de senha de auto-atendimento
- Ferramentas leves de administração de usuários
- Inicialização e monitoração de workflows (caso o Módulo de Aprovisionamento esteja instalado)
- Gerenciamento de tarefas pessoais e/ou em equipe (caso o Módulo de Aprovisionamento esteja instalado)
- Recursos de delegação e proxy

O aplicativo de usuário oferece ao administrador do sistema uma vasta gama de recursos de configuração e administração, incluindo:

- Uma interface que permite a configuração e o gerenciamento de direitos de delegação e proxy
- Acesso a ferramentas de registro e relatórios do Crystal Reports personalizados
- Configuração de workflows baseada em assistentes (caso o Módulo de Aprovisionamento esteja instalado)
- Gerenciamento de workflow (caso o Módulo de Aprovisionamento esteja instalado), incluindo a capacidade de reatribuir ou finalizar workflows em andamento
- Designer baseado no Eclipse para a criação de definições de abstração de diretório e relacionamentos personalizados.

Uma lista mais completa de recursos e funções é exibida na tabela a seguir.

Recurso	Descrição
Ambiente de usuário com interface de usuário para Web extensível, independente do browser, baseado em padrões	O administrador pode mudar layouts de página e a home page padrão, adicionar novas páginas e modificar a aparência geral (temas). O aplicativo de usuário pode ser expandido por meio da adição de portlets compatíveis com JSR-168

Recurso	Descrição
Aprovisionamento de workflows (caso o Módulo de Aprovisionamento esteja instalado)	O administrador pode criar workflows personalizados para o processamento de solicitações de aprovisionamento. Esses workflows podem, em seguida, ser iniciados por usuários finais com direitos apropriados.
Workflows orientados por evento (caso o Módulo de Aprovisionamento esteja instalado)	Além dos workflows iniciados por usuário, o administrador pode configurar workflows de modo que sejam ativados automaticamente quando ocorrerem determinados eventos no cofre de identidade.
White pages aprimoradas	Exiba informações de usuário em ordem alfabética, por região, por conjunto de habilidades e assim por diante.
Organograma	O aplicativo de usuário inclui um portlet de organograma avançado que utiliza o AJAX para proporcionar uma experiência altamente interativa.
Pesquisa do usuário	O usuário pode realizar pesquisas de identidades e gravar definições de pesquisa personalizadas para uso posterior.
Auto-atendimento de senha	O aplicativo de usuário permite que usuários finais acessem as funções de gerenciamento de senhas, eliminando as chamadas ao Suporte Técnico.
Administração de usuários parcial	O aplicativo de usuário permite que usuários finais que não sejam administradores de TI realizem um conjunto limitado de tarefas de gerenciamento de identidade.
Designer baseado no Eclipse	Administradores do sistema, desenvolvedores, consultores e outros especialistas de TI podem realizar diversas tarefas de configuração, entre outras, de modo rápido e fácil usando o aplicativo Designer. Por exemplo, o Designer permite trabalhar off-line com relacionamentos e definições de entidades, filtros e políticas de driver, além de várias outras tarefas de configuração relacionadas a ou definidas por driver. As mudanças podem ser gravadas em um projeto e/ou carregadas no cofre de identidade.
Funções de proxy (caso o Módulo de Aprovisionamento esteja instalado)	A interface de usuário do aplicativo permite que indivíduos com direitos apropriados definam funções de proxy para determinados usuários. (Um proxy pode realizar tarefas em nome de outro usuário, tendo todos os direitos daquele usuário.)
Delegação de tarefas (caso o Módulo de Aprovisionamento esteja instalado)	A interface de usuário permite que gerentes (e usuários com direitos apropriados) configurem a delegação automática de tarefas a outros colegas com base na indisponibilidade de determinado usuário. A delegação pode ser ajustada de forma que tipos específicos de tarefas possam ser delegados a diferentes indivíduos.

Recurso	Descrição
Camada de abstração de diretório	A estrutura em tempo de execução isola a lógica de aplicativo Web do funcionamento básico do acesso ao cofre de identidade e workflow, oferecendo assim uma arquitetura de abstração de diretório segura e robusta. O isolamento é possível por meio de uma camada intermediária conhecida como camada de abstração de diretório (ou apenas camada de abstração).
Controle de acesso a todos os dados disponíveis a usuários	A camada de abstração (que tira proveito do sofisticado modelo Direitos Efetivos do eDirectory) limita automaticamente a visibilidade de workflows e dados de identidade, bem como os direitos do usuário de modificar dados, de tal forma que seja transparente ao usuário e até mesmo aos próprios portlets.
Verificação de dados de identidade do usuário final	O aplicativo de usuário fornece aos usuários um modo de ver e validar/atualizar suas próprias informações de identidade da maneira como são representadas no cofre de identidade.
Registro flexível	Registre facilmente diversos eventos em um registro do servidor (por meio do log4j), no Novell Audit, ou em ambos.
Relatórios do Novell Audit	O produto inclui Crystal Reports com gabaritos predefinidos que refletem tarefas comuns de criação de relatório relacionadas ao aprovisionamento.
Alta disponibilidade	O aplicativo de usuário e os elementos de fluxo de aprovação do produto podem ser agrupados em cluster para proporcionar escalabilidade. **Importante:** Nesta versão do Módulo de Aprovisionamento, não há suporte para o failover de instâncias de workflow em andamento. Contudo, um fluxo em processamento que tenha sido interrompido poderá ser concluído em nós do servidor remanescentes por meio de uma etapa de intervenção manual.
IU de gerenciamento de gabarito de e-mail	Associe e personalize gabaritos de e-mail para workflows usando o iManager.
Portlets adicionais	Diversos portlets prontos para o uso são fornecidos com o aplicativo de usuário, incluindo portlets para GroupWise, Exchange, Lotus Notes, Web-mail, Network File, NetStorage, HTML, atalhos, RSS e mensagens

Esses recursos complementam as funções padrão oferecidas pelo Identity Manager. Consulte o *Guia do Administrador do Identity Manager* para obter mais informações sobre o conjunto de recursos padrão do produto.

1.1 Tipos de funções suportadas

O aplicativo de usuário do Identity Manager inclui uma ampla seleção de recursos de gerenciamento de identidade. É possível que nem todos os recursos devam ser usados por (ou estejam visíveis a) todos os usuários; os recursos dependerão da função de cada pessoa.

Os usuários são classificados de acordo com uma ou mais das categorias a seguir, cada uma delas associada a um conjunto diferente de ferramentas e recursos. (O vocabulário a seguir será adotado em toda esta documentação.)

1.1.1 Administrador do LDAP:

O administrador do LDAP é a pessoa com os direitos máximos sobre a configuração e a administração do sistema associadas ao cofre de identidade (eDirectory 8.7.x ou 8.8). Essa é uma função lógica que pode ser compartilhada também pelo Administrador de Aplicativo de Usuário (abaixo), que é a pessoa ou entidade com direitos de sistema ao servidor de aplicativos (JBoss), ao banco de dados (por exemplo, MySQL) e/ou à própria IU da Web baseada em portal.

O administrador do LDAP pode escolher entre dois tipos de ferramentas para realizar seu trabalho: o Designer do Identity Manager baseado no Eclipse para tarefas raras (possivelmente realizadas apenas uma vez), e as ferramentas do iManager para tarefas administrativas diárias.

Tarefas raras que costumam ser realizadas com o Designer do Identity Manager:

- Configuração das definições da camada de abstração, atributos e relacionamentos que podem ser usados no aplicativo de usuário do Identity Manager. Para obter mais informações, consulte o Capítulo 4, “Configurando a Camada de Abstração do Diretório” na página 75.
- Validação das definições da camada de abstração do diretório. (Consulte o Capítulo 4, “Configurando a Camada de Abstração do Diretório” na página 75.)
- Mudanças nas configurações do Driver de Aplicativo do Usuário. (Consulte o Capítulo 3, “Configurando o Driver de Aplicativo do Usuário” na página 57.)
- Localização do texto de exibição para rótulos de entidades e atributos, nomes de relacionamentos em organogramas e itens de listas locais e globais. (Consulte o Capítulo 4, “Configurando a Camada de Abstração do Diretório” na página 75.)
- Importação ou exportação do Driver de Aplicativo do Usuário e suas configurações.
- Outros tipos de tarefas off-line.

Tarefas diárias que o administrador (o Administrador do LDAP ou o Administrador de Aplicativo de Usuário, descrito abaixo) geralmente executa em um sistema em produção são realizadas no iManager. Essas tarefas podem incluir:

- Gerenciamento de gabaritos de e-mail
- Definição ou designação de recursos aprovisionados e definições de solicitação de aprovisionamento.
- Habilitação ou desabilitação de uma definição de workflow, tornando-a ativa ou não.
- Finalização de um workflow em andamento.
- Geração de relatórios com os dados de registro do Novell Audit.

Algumas dessas tarefas (aquelas relacionadas a workflow) são pertinentes apenas quando o Módulo de Aprovisionamento está instalado. Além disso, muitas delas podem ser realizadas pelo Administrador de Aplicativo de Usuário (abaixo) em vez do Administrador do LDAP.

1.1.2 Administrador de Aplicativo de Usuário

O Administrador de Aplicativo de Usuário realiza tarefas associadas à administração do aplicativo Web (o aplicativo baseado em browser que é executado no JBoss). O acesso às ferramentas de administração dessa função ocorre por meio da guia Administração da interface de usuário do Identity Manager.

A seguir estão algumas das ações que você pode executar no aplicativo de usuário

- Configuração de várias definições de aplicativo, como aquelas que informam ao aplicativo de usuário como se conectar ao cofre de identidade (provedor do LDAP). Para obter detalhes, consulte o Capítulo 10, “Configuração do portal” na página 199.
- Determinação das páginas exibidas na interface de usuário do Identity Manager e de quem tem permissão para acessá-las. (Consulte o Capítulo 7, “Administração de Página” na página 137.)
- Determinação dos portlets exibidos na interface de usuário do Identity Manager e de quem tem permissão para acessá-los. (Consulte o Capítulo 9, “Administração de Portlet” na página 179.)
- Determinação da aparência da interface de usuário do Identity Manager. (Consulte o Capítulo 8, “Configuração de tema” na página 173.)
- Controle dos níveis de mensagens de registro que você deseja que o aplicativo de usuário do Identity Manager crie, e quais dessas mensagens (se houver) serão enviadas ao Novell Audit. (Consulte o Capítulo 12, “Configuração de Registro” na página 211.)
- Gerenciamento dos diversos caches mantidos pelo aplicativo de usuário do Identity Manager. (Consulte o Capítulo 13, “Configuração de cache” na página 217.)
- Exportação ou importação do conteúdo da Web (páginas e portlets) usado no aplicativo de usuário do Identity Manager. (Consulte o Capítulo 14, “Ferramentas para a exportação e a importação de dados de portal” na página 227.)
- Configuração de direitos de proxy para determinados indivíduos.
- Várias outras tarefas relacionadas à interface de usuário exibida para o usuário final.

A seguir estão tarefas que são realizadas no iManager:

- Gerenciamento de gabaritos de e-mail
- Definição ou designação de recursos aprovisionados e definições de solicitação de aprovisionamento.
- Habilitação ou desabilitação de uma definição de workflow, tornando-a ativa ou não.
- Finalização de um workflow em andamento.
- Geração de relatórios com os dados de registro do Novell Audit.

Algumas dessas tarefas (aquelas relacionadas a workflow) são pertinentes apenas quando o Módulo de Aprovisionamento está instalado.

1.1.3 Usuário final

O usuário final é a pessoa que vê e interage com os diversos portlets e páginas da Web que, juntos, formam a interface de usuário do aplicativo de usuário. Nesse contexto, o usuário final indica um funcionário, um gerente ou alguém (proxy) a quem um funcionário ou gerente delega suas próprias funções.

O usuário final usufrui potencialmente de uma ampla gama de recursos, dependendo do que tiver sido habilitado pelo administrador. No mínimo, os usuários finais poderão usar o aplicativo de usuário do Identity Manager para:

- Ver os relacionamentos hierárquicos entre objetos Usuário utilizando o portlet Organograma.
- Ver e editar informações de usuário (de acordo com os direitos apropriados).
- Pesquisar usuários ou recursos usando critérios de pesquisa avançados (que podem ser gravados para uso posterior).
- Recuperar senhas esquecidas.
- Enviar e-mails a membros da equipe (individual ou globalmente).

Além disso, com o Módulo de Aprovisionamento instalado, a interface da Web do aplicativo de usuário permite aos usuários:

- Solicitar um recurso (iniciar um dos diversos workflows possivelmente predefinidos).
- Ver o status de solicitações passadas.
- Reivindicar tarefas e ver listas de tarefas (por recurso, destinatário ou outras características).
- Ver atribuições de proxy.
- Ver atribuições delegadas.
- Especificar sua própria (in)disponibilidade.
- Entrar no modo proxy a fim de reivindicar tarefas em nome de outros usuários.
- Ver tarefas de equipe, solicitar recursos de equipe e assim por diante (apenas os gerentes).



1.1.4 Usuário indicado

Um usuário indicado (ou apenas indicado) é um usuário final a quem uma ou mais tarefas específicas (apropriadas aos direitos desse usuário) podem ser delegadas, para que ele possa trabalhar em tais tarefas em nome de outra pessoa. Por exemplo, João sairá de férias e deseja que Maria lide com suas tarefas enquanto ele estiver fora. Contanto que Maria tenha os direitos apropriados para realizar a(s) tarefa(s) delegada(s) por João, ela poderá tornar-se delegada de João. Quando João indicar que não está disponível no aplicativo de usuário, as tarefas que normalmente seriam exibidas na lista de tarefas de João serão exibidas na lista de tarefas de Maria. Desse modo, Maria terá a função de usuário indicado. Ela poderá reivindicar uma tarefa de João como se fosse totalmente sua (e não mais de João). Compare esse item com a definição de usuário proxy descrita abaixo.

Observe que a delegação ocorre de acordo com cada tarefa. Não é necessariamente uma transferência total de responsabilidades (embora, na verdade, a interface de usuário permita a delegação global de todas as tarefas de um usuário a um delegado específico, se necessário). Um usuário pode designar mais de um delegado. Cada delegado só pode ser responsável pela(s) tarefa(s) que lhe for(em) concedida(s). (Por exemplo, João deseja que Maria lide com todas as tarefas relacionadas a novas solicitações de cartão comercial recebidas, porém deseja que Pedro lide com novas solicitações de contas Siebel.) A transferência de responsabilidade – a designação de novas tarefas – acontece automaticamente assim que o proprietário original da tarefa declara não estar disponível para um determinado tipo de tarefa. (O declarante pode, opcionalmente, especificar um período de expiração da delegação, e isso pode ser feito para cada tarefa específica). Essa transferência é registrada por razões de conformidade.

Uma descrição detalhada dos recursos da interface de usuário para usuários delegados pode ser encontrada no Capítulo 1 do *Aplicativo de usuário do Identity Manager: Guia do Usuário*. Consulte também a Seção 21.3, “Segurança de aprovisionamento” na página 317 neste guia.

1.1.5 Usuário proxy

Um usuário proxy é um usuário final que age em nome de outro usuário assumindo sua identidade temporariamente. Todos os direitos do usuário original passam ao proxy. O trabalho do usuário original continua a ser de sua propriedade. Por exemplo, enquanto João estiver viajando pela China, ele deseja que seu assistente administrativo, Paulo, possa acessar e agir em seu nome em relação a todas as suas tarefas (de João). Caso João tenha os direitos apropriados, poderá designar Paulo como seu proxy. (Se ele não tiver os direitos apropriados, o Administrador do Aplicativo de Usuário configurará essa opção.) Uma vez estabelecido o relacionamento de proxy, Paulo poderá ter duas funções: a sua própria função e a função de João. Ele poderá fazer tudo o que a função de João permite fazer. Quando itens de trabalho forem realizados por Paulo, será como se tivessem sido realizados por João.

Observe que, em comparação com o mecanismo de delegação descrito na seção anterior, um relacionamento de proxy concede ao proxy visibilidade total (e poder de agir) em relação às tarefas e configurações do usuário original. Além disso, os atributos, relacionamentos ou configurações do sistema aos quais João tem acesso estarão acessíveis para seu proxy, enquanto durar a função de proxy.

Outra diferença entre um delegado e um proxy é o fato de que o usuário pode delegar algumas tarefas a um delegado e outra categoria de tarefas a outro delegado, ao passo que um proxy sempre recebe todas as tarefas do usuário original. Em outras palavras, ao nomear uma pessoa como seu

proxy, você poderá ter certeza de que todas as suas tarefas serão vistas e realizadas por aquele indivíduo. É como se o indivíduo em questão tivesse tomado seu lugar.

Observe que ações de proxy realizadas em nome de outro usuário são registradas no Novell Audit (com o propósito de demonstração de conformidade).

Informações adicionais sobre situações de uso de proxy podem ser encontradas em "Definindo as configurações de aprovisionamento" do *Aplicativo de Usuário do Identity Manager: Guia do Usuário*.

1.2 Abstração de dados: a chave para o gerenciamento de identidades flexível

O conceito de abstração de dados (a capacidade de definir, ver e manipular instâncias de definições da camada de abstração de diretório) é fundamental para o entendimento do aplicativo de usuário do Identity Manager.

A tecnologia de armazenamento tradicional envolve bancos de dados relacionais, diretórios X.500 ou outros repositórios, e geralmente requer que entradas de dados (linhas em um banco de dados, objetos em um diretório X.500 e assim por diante) obedeçam totalmente a um esquema bem definido. As consultas a dados armazenados podem ser arbitrariamente complexas (em teoria) e os dados podem incluir índices e/ou backlinks, mas as próprias entradas de dados devem obedecer a uma definição fixa. Além disso, elas presumem que os esquemas aplicáveis não serão mudados de modo significativo, ou nunca serão mudados, com o passar do tempo.

Isso causa problemas quando as informações (possivelmente originárias de diferentes fontes de dados com esquemas distintos) têm de ser reunidas para criar objetos de dados compostos que obedeçam a um esquema novo (e talvez temporário). Dados de identidade são um exemplo clássico dessa situação, pois tendem a não ser compostos nem estáticos. Além disso, os dados nos quais uma determinada identidade se baseia podem ser originários de diferentes fontes, cada uma com um administrador interessado em proteger suas informações (obviamente).

A natureza distribuída dos dados de identidade cria vários desafios ao gerenciamento de identidades, que podem ser difíceis de superar devido a definições de esquema rígidas (e limitadas por políticas) Um modo de enfrentar o problema é unir os dados de identidade em um cofre de identidade lógico (implementado como um diretório) e construir as identidades lógicas usando os dados de origem, conforme for necessário, de acordo com um ou mais esquemas lógicos que associem objetos e atributos LDAP tradicionais (por exemplo) a atributos e definições da camada de abstração arbitrários. Assim, os dados de identidade podem ser usados em composições e tornam-se altamente dinâmicos A mudança da definição de uma identidade não requer mudanças em um esquema LDAP. Objetos de identidade podem ser redefinidos sempre que necessário, para se adequarem a aplicações ou até mesmo a usuários específicos de determinados aplicativos.

Essa abordagem geral é geralmente chamada de abstração de dados, o que significa que identidades são materializadas conforme necessário e no formato exigido.

A abstração de dados de identidade apresenta diversas vantagens:

- É possível evitar mudanças que interrompam ou coloquem em risco os esquemas de diretórios LDAP
- A tecnologia de abstração não é intrusiva e não exige que sejam feitas mudanças nos sistemas conectados
- É possível a ocorrência de novos relacionamentos entre dados

- As definições da camada de abstração podem ser mudadas ou expandidas a qualquer momento
- Os objetos podem ter muitos ou poucos atributos, conforme necessário
- Atributos de classes de objetos LDAP não relacionadas podem ser fundidos na definição da camada de abstração
- Nomes arbitrários podem ser usados para a nomeação de atributos (não é obrigatório o uso de nomes LDAP)
- É possível manter políticas minuciosas de controle de acesso (os usuários vêem apenas os dados aos quais têm direito)
- É possível realizar pesquisas complexas em relação a novos tipos de objetos (ou combinações de atributos) que não seriam possíveis em um ambiente puramente LDAP

O Identity Manager tira proveito da abstração para alcançar todos esses objetivos e muito mais.

1.3 Visão geral de alto nível da arquitetura

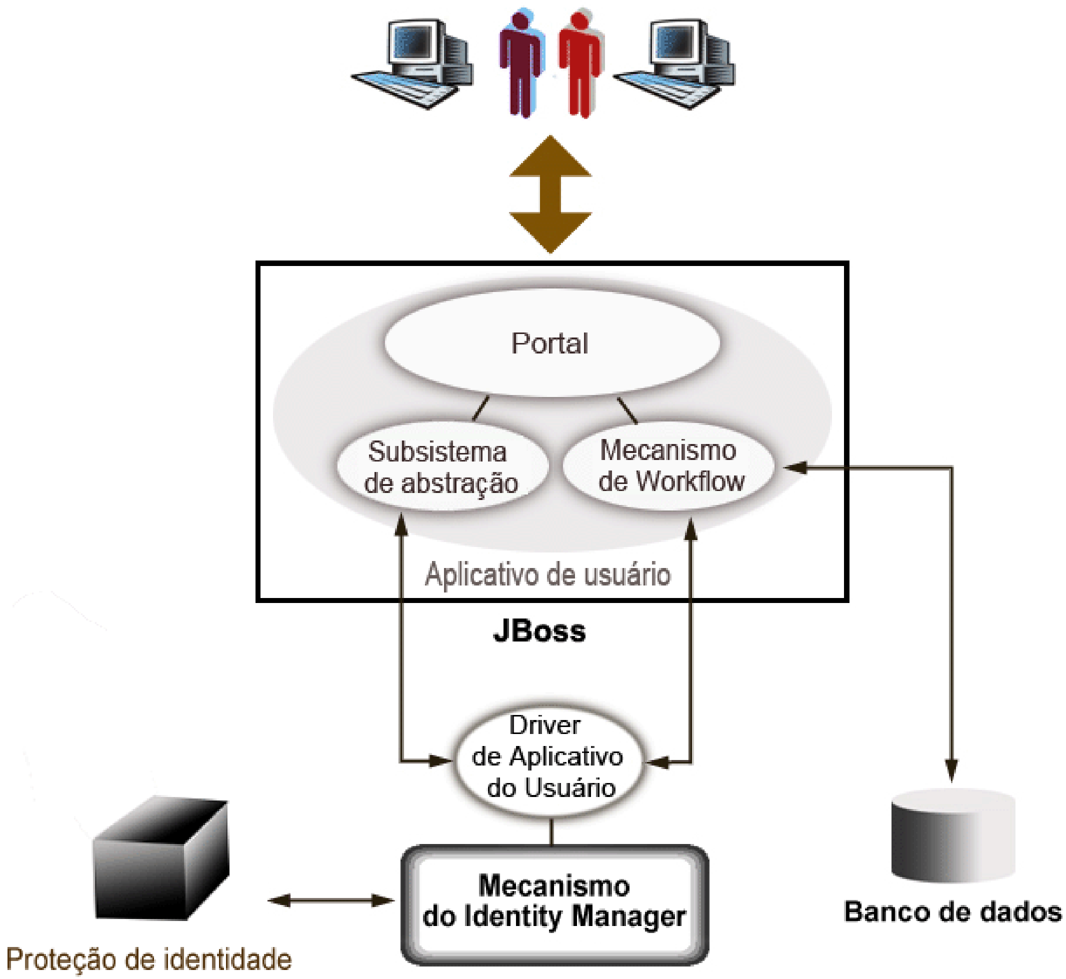
O aplicativo de usuário do Identity Manager depende de diversos componentes independentes que funcionam em conjunto. Os componentes básicos e suas responsabilidades fundamentais estão descritos na tabela a seguir.

Componente	Descrição
Cofre de identidade (eDirectory 8.7.3 ou 8.8)	O repositório para dados de usuário (e outros dados de identidade), o conjunto de driver e os drivers do IDM, bem como vários artefatos da camada de abstração e (caso o Módulo de Aprovisionamento esteja instalado) os artefatos de workflow.
Mecanismo do Identity Manager	Esse é a estrutura de tempo de execução do Identity Manager que monitora eventos no eDirectory (e em outros sistemas conectados), assegurando o uso obrigatório de políticas e roteando dados de entrada e saída do cofre de identidade.
Driver de Aplicativo do Usuário	O Driver de Aplicativo do Usuário comunica-se com o aplicativo de usuário para permitir que ele atualize seu cache quando as definições da camada de abstração são mudadas. Quando o Módulo de Aprovisionamento está instalado, o Driver de Aplicativo do Usuário também pode ser configurado para permitir eventos nos workflows de acionadores do cofre de identidade. Ele também envia informações sobre direitos ao cofre de identidade, de modo que haja um registro da concessão (ou não) do direito quando o workflow for concluído.
Aplicativo de usuário: IU da Web	A IU da Web do aplicativo de usuário é um aplicativo Java baseado em browser ao qual são conectados os portlets compatíveis com JSR 168.
Aplicativo de usuário: Camada de Abstração	A camada de abstração isola o cofre de identidade da lógica de camada de apresentação, assim, todas as solicitações de dados de identidade são encaminhadas através da camada de abstração. O código do portlet não pode obter acesso direto às informações de identidade. Todas as solicitações passam pela camada de abstração e estão sujeitas aos seus limites (de controle de acesso, por exemplo).

Componente	Descrição
Aplicativo de usuário: Mecanismo de Workflow (disponível apenas quando o Módulo de Aprovisionamento está instalado)	O Mecanismo de Workflow é um conjunto de arquivos Java executáveis responsável pelo gerenciamento e execução de etapas em um workflow definido pelo administrador.
Servidor de aplicativos JBoss	O servidor de aplicativos de código-fonte aberto JBoss fornece a estrutura de tempo de execução na qual o aplicativo de usuário, a camada de abstração e o Mecanismo de Workflow são executados.
Banco de dados (MySQL por padrão)	O banco de dados (consulte o Guia de Instalação para obter uma lista dos bancos de dados com suporte) armazena certos tipos de informações de configuração em nome do aplicativo de usuário, bem como o estado do workflow (caso o Módulo de Aprovisionamento esteja instalado).
Driver de serviço Composer	O Driver de serviço Composer é a parte do Driver de Aplicativo do Usuário que pode ser configurada de modo personalizado para responder a eventos do cofre de identidade acionando workflows.
Novell Audit	O Novell Audit é um servidor de registro independente que pode manter diversos tipos de dados (como dados gerados pelas etapas de um workflow). Para obter mais informações, consulte o capítulo sobre a configuração do registro, mais adiante neste manual.

Em termos de fluxo de informações, os componentes mencionados acima estão vinculados de modo lógico da maneira ilustrada no diagrama a seguir. Os componentes individuais podem estar (e, na maioria dos casos, estarão) fisicamente localizados em mais de uma máquina. Por exemplo, embora o cofre de identidade (e sua principal ferramenta de administração, o iManager) esteja localizado na máquina que hospeda o mecanismo do Identity Manager, o JBoss (e o aplicativo de usuário) estarão geralmente localizados em uma máquina separada (ou em um grupo de máquinas, caso sejam usados clusters). Da mesma forma, não apenas por questões de desempenho, mas também de segurança e

recuperação de desastres, o banco de dados (MySQL) geralmente está instalado em uma máquina própria.



1.3.1 Cofre de identidade

O cofre de identidade é usado para armazenar dados de identidade e definições da camada de abstração de diversos tipos. Uma instância do eDirectory (executada no Windows, Solaris ou Linux) é usada para esse fim. Usando o eDirectory, o Identity Manager pode tirar proveito do diretório LDAPv3, um diretório comprovado de classe empresarial e escalável, com recursos de particionamento e replicação, além de uma ferramenta flexível de configuração e gerenciamento baseada na Web (iManager) que oferece um ponto de integração administrativa completo entre o Identity Manager e o próprio eDirectory.

1.3.2 JBoss

O aplicativo de usuário é fornecido em um pacote como um arquivo de aplicativo Java Web, ou arquivo WAR (Web Application Archive). O arquivo WAR é distribuído ao JBoss, o popular servidor de aplicativos Java de código-fonte aberto (que usa o Tomcat como seu mecanismo de

servlet; não mostrado no diagrama). O uso do JBoss como um ambiente de execução traz diversas vantagens, dentre elas:

- O código-fonte está livremente disponível.
- O JBoss pode ser implementado em cluster a partir da versão 4.0.3.
- O JBoss é totalmente compatível com J2EE, o que significa que aplicativos J2EE podem ser executados nele. Aplicativos adicionais (por exemplo, Serviços Web) podem ser executados na mesma instância do JBoss usada pelo aplicativo de usuário.
- O JBoss oferece suporte a serviços de autorização e segurança Java JAAS e JACC padrão (dos quais o aplicativo de usuário depende para o acesso ao cofre de identidade).
- O JBoss pode ser executado em diversas plataformas, incluindo versões populares do Windows e Linux.

O WAR do aplicativo de usuário contém código executável para o aplicativo de usuário, que, por sua vez, é criado usando a arquitetura MVC (Model-View-Controller), a fim de separar os componentes. A interface do usuário é executada como portlets modulares no aplicativo de usuário. Há portlets separados para a exibição de organogramas, a realização de pesquisas, a exibição de detalhes de usuários, a redefinição de senhas e assim por diante.

Para obter mais informações sobre os diversos aspectos da distribuição de aplicativos Web ao JBoss, consulte a documentação do JBoss em http://www.jboss.org/products/jbossas/docs (http://www.jboss.org/products/jbossas/docs).

1.3.3 Banco de Dados

O aplicativo de usuário depende de um banco de dados (por padrão, MySQL; consulte o Guia de Instalação para obter uma lista dos banco de dados com suporte) para armazenar diversos tipos de informações:

- Dados de configuração do aplicativo de usuário: por exemplo, definições de página da Web, registros de instâncias de portlet e valores preferenciais.
- Se o Módulo de Aprovisionamento estiver instalado, as informações de estado de workflow serão mantidas no banco de dados. (As definições de workflow reais serão armazenadas no cofre de identidade.)
- Registros do Novell Audit

1.3.4 Mecanismo do Identity Manager

O produto Identity Manager consiste em um mecanismo de tempo de execução, drivers e políticas. O mecanismo do Identity Manager responde a eventos no cofre de identidade e gerencia o fluxo e a transformação de dados de entrada e saída do cofre de identidade. Objetos driver contêm código executável e artefatos (como documentos de política) projetados para proporcionar comportamentos de manipulação de dados específicos a um determinado sistema conectado. O aplicativo de usuário do Identity Manager é um sistema conectado. A comunicação entre o cofre de identidade, a camada de abstração do aplicativo de usuário e o Mecanismo de Workflow ocorre por meio do Driver de Aplicativo do Usuário (veja abaixo).

Como o aplicativo de usuário depende de diversos objetos diretório para o armazenamento de artefatos da camada de abstração, é necessário expandir o esquema do eDirectory para acomodar objetos e atributos LDAP personalizados necessários ao aplicativo de usuário. A expansão do

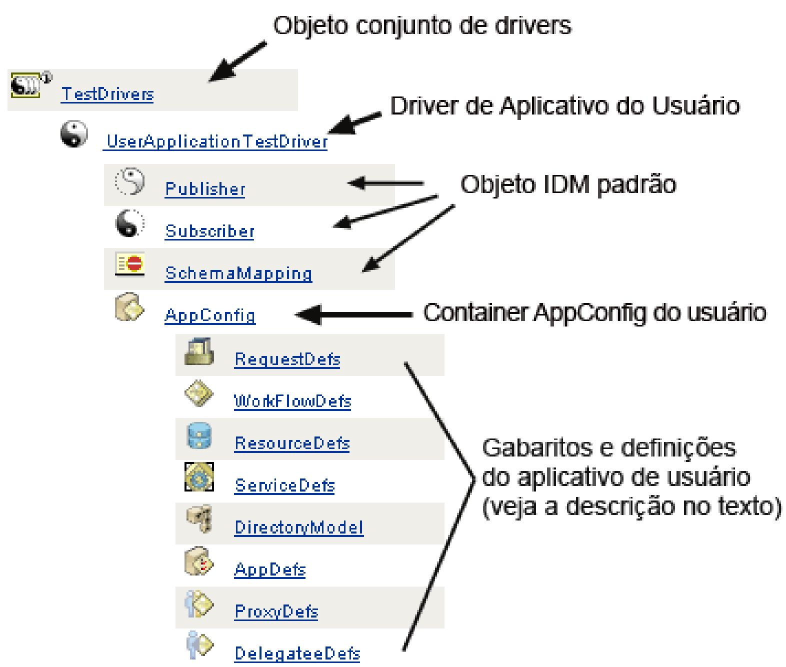
esquema ocorre automaticamente como parte do processo de instalação do Identity Manager. Contudo, o preenchimento com objetos e atributos personalizados com valores padrão só ocorre depois que o Driver de Aplicativo do Usuário é instalado e ativado.

1.3.5 Driver de Aplicativo do Usuário

O Driver de Aplicativo do Usuário é um componente essencial do aplicativo de usuário. Uma das responsabilidades do Driver de Aplicativo do Usuário é notificar a camada de abstração quando valores de dados importantes são mudados no cofre de identidade, de modo que a camada de abstração saiba que deve atualizar seu cache.

Se o Módulo de Aprovisionamento estiver instalado, o Driver de Aplicativo do Usuário poderá ser configurado para acionar automaticamente os workflows em resposta a mudanças nos valores de atributo no cofre de identidade.

O Driver de Aplicativo do Usuário não é apenas um componente de tempo de execução, mas também um agrupador de armazenamento para objetos diretório (englobando os artefatos de tempo de execução do aplicativo de usuário). A seguir está uma representação típica de artefatos de diretório associados ao Driver de Aplicativo do Usuário.



Observação: Os nomes mostrados representam valores de nome comum (cn) do LDAP. A nomeação de esquema real de diversas classes de objetos é abordada em outra parte.

Essas categorias de artefatos são abordadas com mais detalhes abaixo.

Objeto conjunto de drivers

Todas as instalações do Identity Manager exigem que os drivers sejam agrupados em conjuntos de drivers. Apenas um conjunto de drivers pode estar ativo por vez (em um determinado servidor de diretório). Os drivers naquele conjunto podem ser ativados ou desativados individualmente, sem

afetar o conjunto de drivers como um todo. O Driver de Aplicativo do Usuário (assim como qualquer outro driver IDM) deve existir em um conjunto de drivers. O conjunto de drivers não é criado automaticamente pelo aplicativo de usuário; você deve criá-lo previamente e, em seguida, criar o Driver de Aplicativo do Usuário a ser inserido naquele conjunto.

Driver de Aplicativo do Usuário

O objeto Driver de Aplicativo do Usuário (que pode receber qualquer nome desejado) é o container de diversos artefatos. Assim como todos os drivers do Identity Manager, o Driver de Aplicativo do Usuário implementa os objetos e as políticas dos canais do Editor e do Assinante. O canal do Editor não é usado pelo aplicativo de usuário, embora esteja disponível para cenários com uso personalizado.

Object App Config (0)

O objeto AppConfig é um container para vários objetos de configuração de aplicativo de usuário:

RequestDefs

Esse é um container de Definições de Solicitação de Aprovisionamento, que são as definições de solicitação configuradas pelo administrador disponíveis para o tempo de execução do aplicativo de usuário (caso o Módulo de Aprovisionamento exista). As definições aqui armazenadas (em formato XML) representam as classes de solicitações que podem ser instanciadas por usuários finais com direitos apropriados por meio do aplicativo de usuário. O RequestDef associa um WorkFlowDef (abaixo) a um ResourceDef.

WorkFlowDefs

Um container para objetos Workflow, incluindo descrições de tempo de design e os gabaritos ou fluxos não utilizados.

ResourceDefs

Um container para definições de Recurso Aprovisionado, incluindo descrições de tempo de design e os gabaritos ou destinos não utilizados.

ServiceDefs

Um container para objetos Definição de Serviço, que agrupa Serviços Web chamados pelos Workflows.

DirectoryModel

Objetos de meta-nível da camada de abstração (ChoiceDefs, EntityDefs, RelationshipDefs), que representam diferentes tipos de conteúdo (alguns podem ser definidos pelo usuário e outros são definidos pelo administrador) do diretório que pode ser exposto pelos Portlets de Identidade.

AppDefs

Um container para objetos de configuração usados para inicializar o ambiente de tempo de execução, como as informações de configuração de cache e as propriedades de notificação de e-mail.

ProxyDefs

Um container para definições de proxy.

DelegateeDefs

Um container para definições de delegado.

1.3.6 Camada de abstração de diretório

Os portlets obtêm seus dados de identidade por meio de consultas à camada de abstração de diretório, uma camada de código que isola detalhes do acesso aos dados de identidade dos processos de cliente. Por exemplo, quando um portlet precisa realizar uma pesquisa de dados de identidade, a camada de abstração faz as consultas LDAP apropriadas em nome do portlet, usando para isso o container de destino no cofre de identidade. Um portlet nunca faz consultas diretas no cofre de identidade.

A camada de abstração é também a camada de código mediante a qual são criadas ou mudadas as definições de camada de abstração, conforme especificadas pelos administradores ou outros usuários qualificados do sistema. Para fazer essas mudanças, o especialista em sistema usa o editor da camada de abstração de diretório do aplicativo Designer, descrito mais adiante neste guia em Capítulo 4, "Configurando a Camada de Abstração do Diretório" na página 75.

No tempo de execução, a camada de abstração mantém em cache diversos tipos de dados de configuração e definição de entidade obtidos do cofre de identidade. Os diversos caches mantidos pelo aplicativo de usuário podem ser gerenciados em detalhes pelo administrador. Para obter mais informações sobre caches e gerenciamento de cache, consulte o Capítulo 13, "Configuração de cache" na página 217.

1.3.7 Mecanismo de workflow

O mecanismo de workflow (disponível no Módulo de Aprovisionamento) é o conjunto de classes de tempo de execução responsável pela execução das etapas de um workflow de acordo com uma definição de processo (um artefato de tempo de execução criado quando uma instância de workflow é criada) e pelo monitoramento das informações de estado, que são mantidas em um banco de dados, como MySQL ou Oracle; consulte a Seção 1.3.3, "Banco de Dados" na página 24, acima.

Há detalhes adicionais sobre o sistema de workflow, inclusive a maneira de criar workflows, no capítulo Capítulo 21, "Introdução ao aprovisionamento com base em workflow" na página 307, mais adiante neste guia.

1.3.8 Interface do usuário

A interface do usuário do Identity Manager é composta de um conjunto de portlets compatíveis com JSR168 (e, no caso do Módulo de Aprovisionamento, algumas Páginas do Servidor Java) que é executado em um aplicativo Web Java no JBoss. A arquitetura de portlet proporciona uma ampla utilização de módulos, bem como personalização de conteúdo e controle da aparência da página pelo usuário. A estrutura do aplicativo de usuário fornece serviços de container de diversos tipos. Ela gerencia o estado da janela, as preferências de portlet, a persistência, o armazenamento em cache, os temas, o registro e assim por diante, além de agir como guardião da segurança. O servidor de aplicativos no qual o aplicativo de usuário é executado proporciona vários serviços ao aplicativo

como um todo, como escalabilidade por meio de clusters, acesso ao banco de dados via JDBC e suporte à segurança baseada em certificado.

O alto grau de encapsulação oferecido por essa arquitetura proporciona um ambiente de camada de apresentação seguro e robusto ao aplicativo de usuário do Identity Manager. Ela garante também um alto grau de controle administrativo em relação a todos os aspectos da interface de usuário.

Para obter mais informações sobre a administração dos diversos aspectos da interface de usuário, consulte os vários capítulos da Parte III, “Administrando o aplicativo de usuário” na página 129 deste guia.

1.4 Ferramentas de projeto e configuração

Diversas funções do aplicativo de usuário do Identity Manager podem ser personalizadas ou configuradas com o uso da ferramenta Identity Manager Designer (baseada na plataforma Eclipse Rich Client) ou dos plug-ins do iManager.

As ferramentas disponíveis e seu uso apropriado estão descritos na tabela a seguir.

Ferramenta	**Finalidade**
Designer do Identity Manager	Ferramenta de configuração geral do Identity Manager que permite ao desenvolvedor, consultor ou administrador do sistema implementar mudanças detalhadas na configuração de conjuntos de drivers, definições de políticas e outros artefatos.
Plug-in Editor da camada de abstração de diretório para o Designer	Permite definir objetos e relacionamentos personalizados, bem como fazer mudanças em várias configurações da camada de abstração. Consulte o Capítulo 4, “Configurando a Camada de Abstração do Diretório” na página 75, mais adiante neste guia.
Plug-in Configuração de Solicitação de Aprovisionamento	Permite a definição e a configuração de tipos de solicitação de aprovisionamento disponíveis (no iManager)
Editor de Recursos Aprovisionados (disponível em breve)	Plug-in do Designer que permite a criação e a configuração de recursos (objetos que representam o recurso que será concedido em resposta a um workflow)
Editor de Definições de Workflow (disponível em breve)	Plug-in para definição de workflow gráfico do Designer
Editor de Gabaritos de E-mail de Workflow	Um plug-in do iManager que permite aos administradores adicionar, apagar e editar gabaritos de e-mail. Os gabaritos podem ser usados pelo sistema de workflow para notificar os usuários quanto a eventos de workflow.

Ferramenta	Finalidade
lreport.exe (ferramenta de relatório de registro) e Recurso de Auditoria e Registro do iManager	Diversos relatórios de registro predefinidos (fornecidos com o Identity Manager) estão disponíveis no formato Crystal Reports (.rpt) para a filtragem de dados registrados no banco de dados do Novell Audit. A ferramenta de relatório de registro **lreport.exe** (apenas para Windows) oferece um modo de gerar relatórios. Você também pode usar outros métodos para criar os relatórios; consulte o Capítulo 5, "Configurando o registro" na página 119 para obter detalhes.

Um especialista em projeto de sistema em geral começaria usando o editor da camada de abstração de diretório (no Designer do Identity Manager) para configurar definições da camada de abstração personalizadas para o aplicativo de usuário. Esses objetos tornam-se então disponíveis para o uso pela camada de abstração (e, assim, por usuários da interface de usuário). Ao usar e definir esses objetos, é possível determinar em detalhes as configurações de controle de acesso, de modo que o administrador e os usuários finais possam ver e manipular apenas os objetos (e atributos de objetos) para os quais tenham os direitos apropriados.

Se o Módulo de Aprovisionamento estiver instalado, o especialista em projeto de sistema poderá usar os assistentes de Configuração de Solicitação de Aprovisionamento do iManager para definir os recursos e workflows aprovisionados que estarão disponíveis aos usuários do aplicativo de usuário. Ao mesmo tempo, o administrador poderá usar a função de editor de gabaritos de e-mail (do iManager) para definir o conteúdo do corpo das notificações de e-mail que serão enviadas pelo(s) workflow(s). Consulte o Capítulo 23, "Gerenciando workflows de aprovisionamento" na página 343 para obter mais informações sobre esse assunto.

Após configurar a camada de abstração, definições de solicitação de aprovisionamento, requisitos de auditoria e gabaritos de e-mail, o administrador geralmente realiza várias operações de configuração que afetam o aplicativo de usuário (envolvendo a segurança, armazenamento em cache e outras funções), usando para isso os recursos de administração descritos em Capítulo 10, "Configuração do portal" na página 199. Por fim, o administrador poderá configurar os portlets individuais conforme necessário, usando as interfaces descritas nos diversos capítulos da Parte IV deste guia.

Observação: O próximo capítulo descreve algumas dessas tarefas em mais detalhes e deve ser consultado antes da implementação de um ambiente de produção.

1.5 Cenários de uso

Há inúmeras funções disponíveis no aplicativo de usuário do Identity Manager. Alguns exemplos servirão para ilustrar as maneiras como o aplicativo de usuário pode ser usado para solucionar problemas reais.

1.5.1 Cenário A: o usuário procura informações sobre outras pessoas da organização

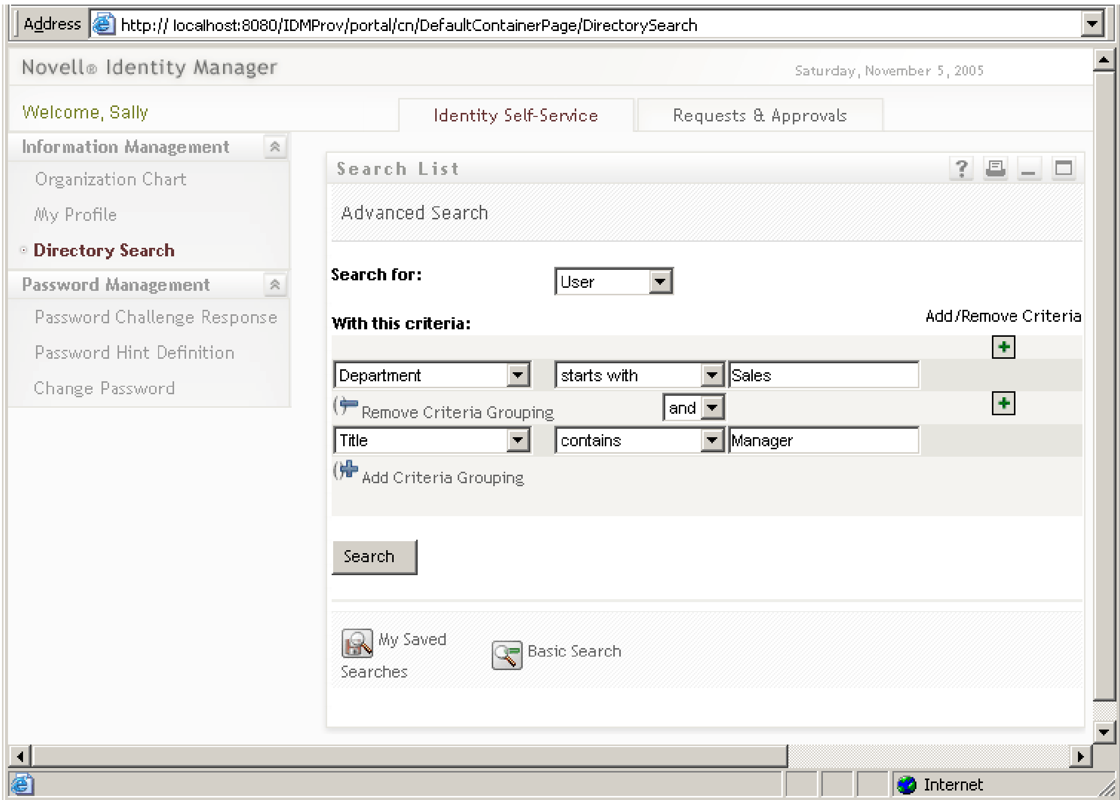
Um caso de uso comum é o de um funcionário que deseja encontrar informações sobre outra pessoa na organização. Por exemplo:

- Obter o nome completo e informações de contato de um colega de trabalho

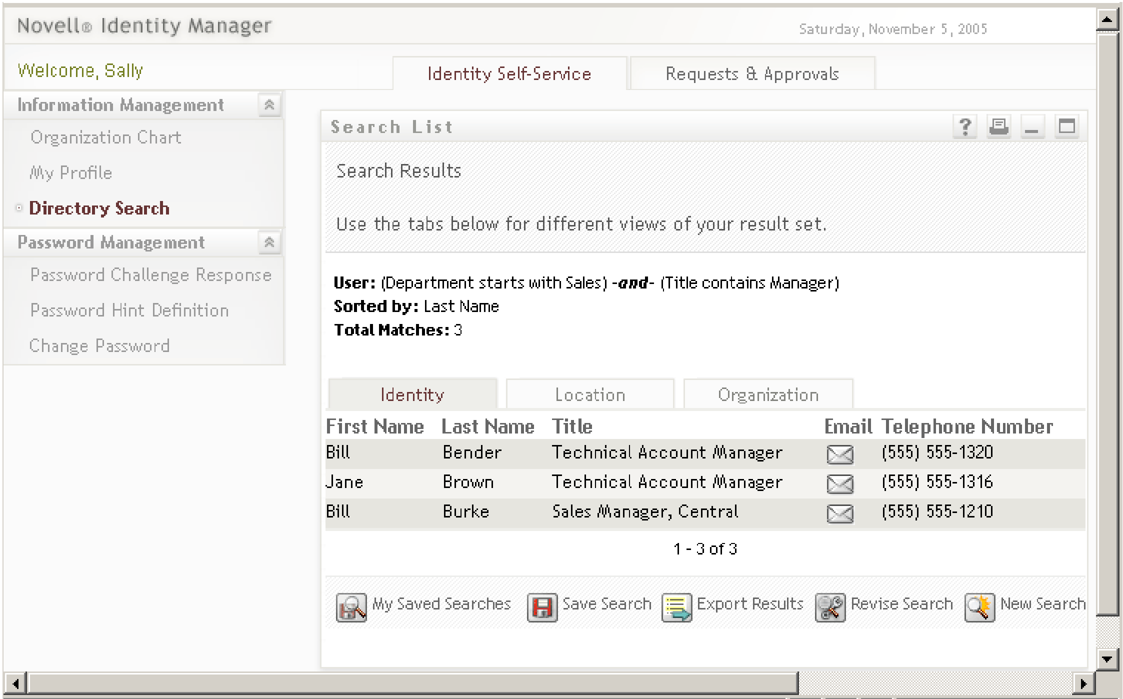
- Encontrar todas as pessoas com determinado conjunto de habilidades em uma localidade
- Determinar quem é o gerente de determinada pessoa

Operações desse tipo (inclusive pesquisas mais avançadas baseadas em consultas complexas) podem ser realizadas facilmente pela interface da Pesquisa de Diretórios. Normalmente, o usuário final efetua login no aplicativo de usuário e acessa a guia Auto-Atendimento de Identidade (caso ela ainda não esteja visível), e clica no link da Pesquisa de Diretórios na coluna de links de navegação à esquerda.

Na tela abaixo, o usuário conectado configurou uma pesquisa avançada para encontrar usuários cujo departamento começa com `Vendas` e cujo `Cargo` contém Gerente.



Quando a pesquisa estiver concluída, a tela de resultados terá a seguinte aparência:

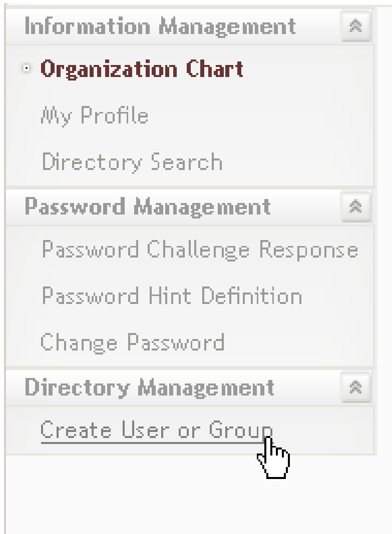


Na parte inferior, observe a fileira de botões que permitem ao usuário gravar essa consulta avançada, verificar a consulta, reiniciar com uma nova pesquisa e assim por diante. Observe também as guias acima da lista das pessoas localizadas. Elas estão relacionadas por Identidade, mas também poderão ser exibidas por Local ou Organização, se você selecionar a guia apropriada.

1.5.2 Cenário B: O gerente cria um novo Usuário

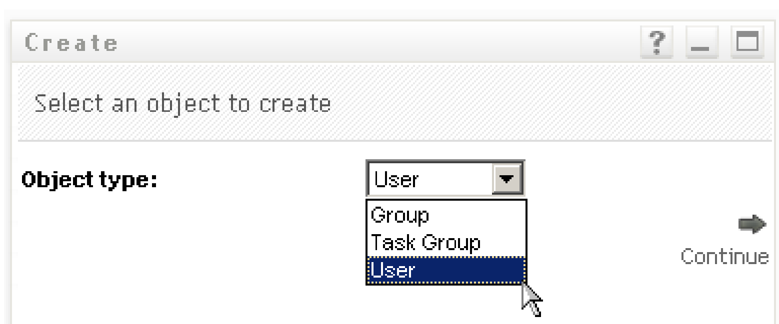
Suponha que um departamento de uma empresa tenha contratado um novo estagiário, prestador de serviço ou outro profissional (que só pode permanecer na empresa por um período fixo). Essa pessoa precisa estar incluída no sistema para que possa receber o conjunto limitado e apropriado de recursos (e ser localizada por pesquisas de Usuário do tipo mencionado acima). Por não ser um funcionário regular, a pessoa não integrará o sistema de Recursos Humanos normal da empresa. No entanto, a identidade dessa pessoa e o seu acesso a recursos precisam ser gerenciados de forma segura.

Como gerente do departamento em questão, você tem autorização para incluir usuários no sistema. Para isso, você efetua login e encontra um link Criar Usuário ou Grupo na coluna de links de navegação à esquerda da página (veja abaixo.):

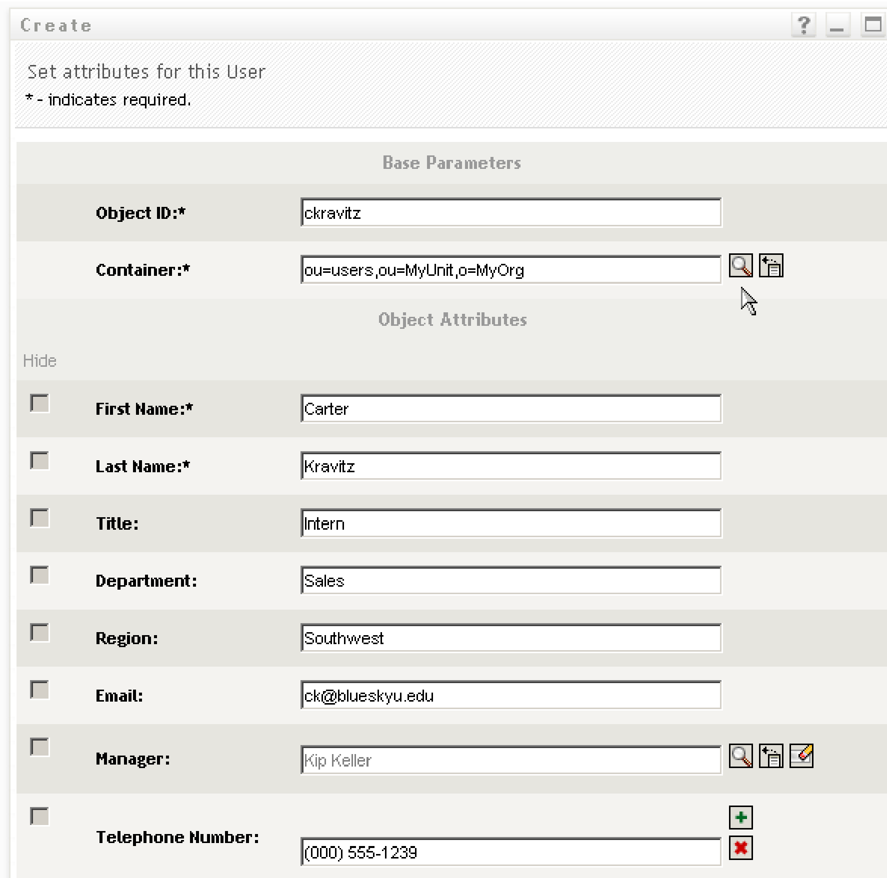


Observação: Esse link só aparecerá se o usuário conectado tiver direitos apropriados.

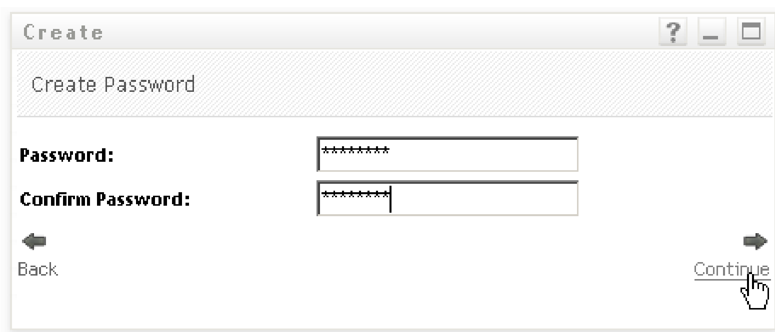
Depois de clicar no link, você terá acesso a uma tela que lhe perguntará se deseja criar um novo Grupo, Tarefa ou Usuário (como indicado abaixo).



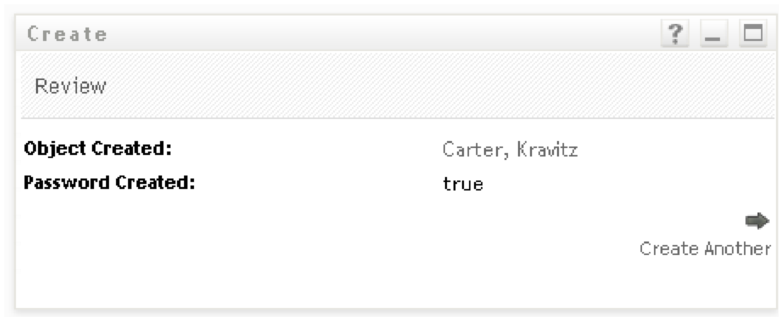
Depois que você selecionar Usuário e clicar em Continuar, poderá digitar informações pessoais do Usuário no próximo painel do assistente:



Na tela seguinte, é possível designar uma senha para o novo Usuário:



A tela final mostra o resultado líquido do processo.



Nesse exemplo, a pessoa recém-incluída torna-se um Usuário com todos os direitos de um Usuário normal. Contudo, é possível definir, por exemplo, um objeto Interno usando o editor da camada de abstração de diretório, com atributos exclusivos e direitos estritamente apropriados ao tipo de objeto. Nesse caso, `Interno` apareceria como uma das opções da lista, junto com Grupo, Grupo de Tarefas e Usuário.

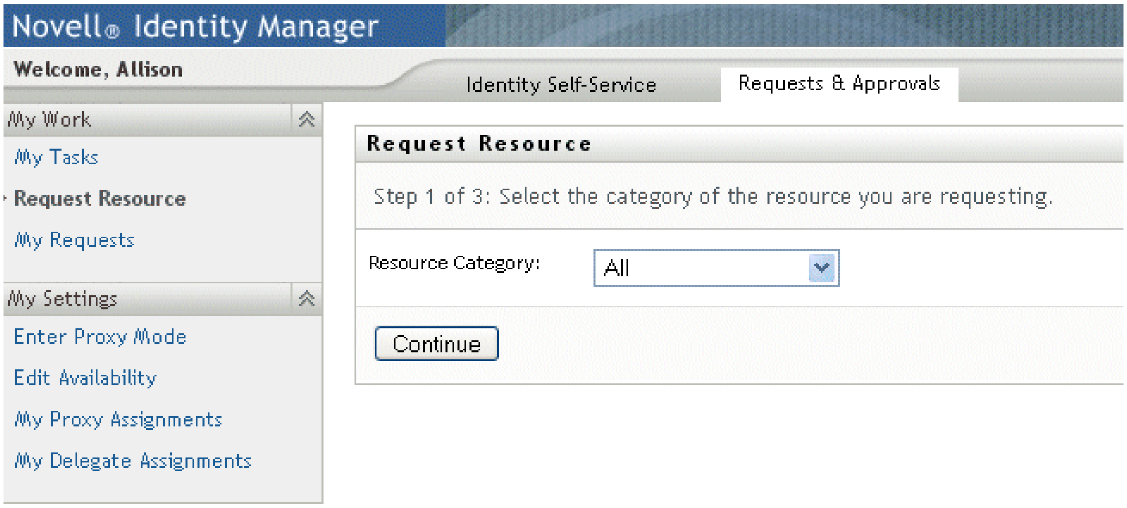
1.5.3 Cenário C: Aprovisionamento de usuário

Uma situação comum é a de um funcionário que precisa obter um recurso (como um equipamento de escritório, um cartão de crédito corporativo ou acesso a um banco de dados) que requer aprovação de outra pessoa. Isso se chama solicitação de aprovisionamento. No Identity Manager, se o Módulo de Aprovisionamento estiver instalado e configurado, essas solicitações poderão ser atendidas mediante workflows.

Observação: Ao contrário dos exemplos anteriores, este exemplo requer que o Módulo de Aprovisionamento esteja instalado e configurado.

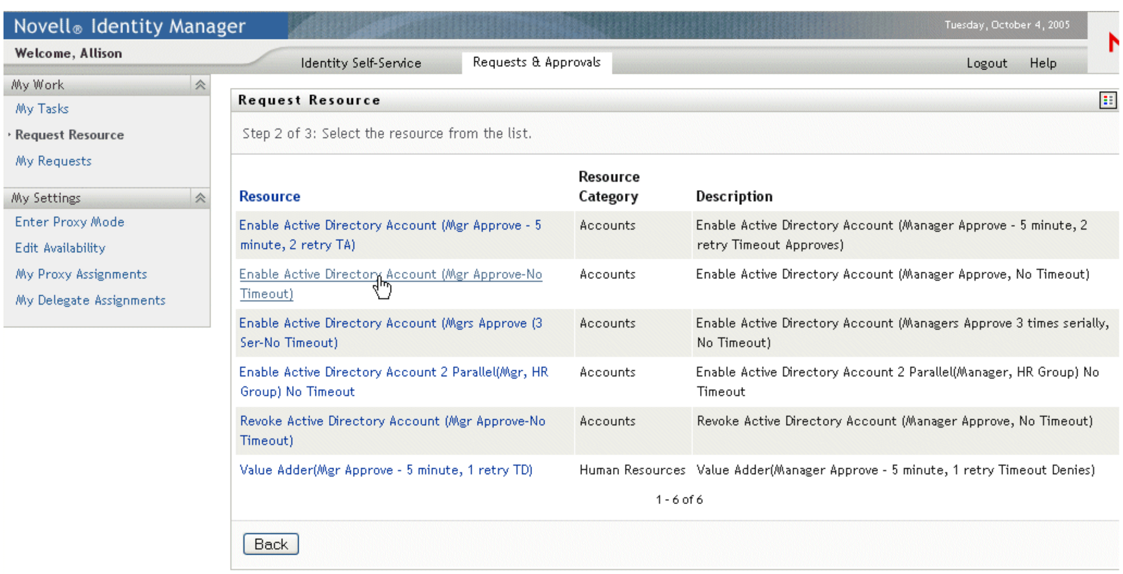
O usuário primeiro efetua login no aplicativo de usuário para acessar sua landing page. No alto da página, o usuário clica na guia *Solicitações e Aprovações* e, em seguida, localiza o *Recurso de*

Solicitação na estrutura de navegação à esquerda. Quando o link *Recurso de Solicitação* é ativado, o aplicativo de usuário exibe o formulário de solicitação inicial.



O menu suspenso Categoria de Recurso pode conter diversos tipos de recurso, inclusive direitos com nomes arbitrários. (Consulte o principal Guia de Administração do Identity Manager para obter mais informações sobre direitos e sobre como eles são criados.) Para ver todos os recursos aprovisionados disponíveis (em outras palavras, tudo o que esse usuário específico, com seus direitos atuais, pode solicitar), basta selecionar `Todos`.

Se o usuário clicar em Continuar, a tela seguinte exibirá todos os tipos de solicitações de aprovisionamento a que o usuário pode ter acesso.



Nesse exemplo, o usuário deseja solicitar uma conta do Active Directory, o que exige a aprovação do gerente. Basta clicar no link apropriado e preencher um formulário simples para que o workflow associado seja ativado e o gerente da pessoa receba uma notificação por e-mail pertinente à tarefa

que o gerente precisa executar. Por sua vez, o gerente pode efetuar login em sua página de *Solicitações e Aprovações* e encontrar a solicitação do funcionário à espera em sua lista de tarefas, pronta para ser aprovada ou negada. (Se o gerente estiver em férias, seu proxy designado será notificado e poderá efetuar login e executar as mesmas ações que o gerente normalmente executaria.) A tela do navegador passa a mostrar uma página de resumo que confirma o sucesso do envio da solicitação de workflow.

A concessão de uma conta em um diretório da empresa (como é mostrado aqui) é um exemplo de uma solicitação de direito. Muitos tipos de solicitações de direito podem ser configurados no aplicativo de usuário do Identity Manager, e diversos tipos de workflows (aprovação de um gerente ou de vários gerentes, fluxo serial ou paralelo, com ou sem tempos de espera, e assim por diante) podem ser criados. Em todos os casos, o controle de acesso estrito está disponível para gerenciar a visibilidade de workflows e outras informações.

Há mais informações sobre esses recursos nos últimos capítulos deste guia. (As informações desses capítulos interessam principalmente a administradores. O uso dos recursos está descrito em mais detalhes no Guia do Usuário do Aplicativo de Usuário do Identity Manager.)

1.6 Próximas etapas

Se você está pronto para saber mais sobre como criar um ambiente de produção, vá para o próximo capítulo (Capítulo 2, "Projetando o ambiente de produção" na página 39). Ou então, consulte um dos últimos capítulos deste manual para obter os seguintes tipos de informação:

Para saber mais sobre os *recursos de registro e auditoria* do aplicativo de usuário, consulte o Capítulo 5, "Configurando o registro" na página 119.

Para saber mais sobre como personalizar a *aparência da interface de usuário*, consulte o Capítulo 8, "Configuração de tema" na página 173.

Para saber mais sobre como a *segurança* é administrada pela interface administrativa do aplicativo de usuário (em comparação com o iManager), consulte o Capítulo 11, "Configuração de segurança" na página 207.

Para saber mais sobre os recursos de *gerenciamento de cache* do aplicativo de usuário, consulte o Capítulo 13, "Configuração de cache" na página 217.

Para saber mais sobre a função de *gerenciamento de senha*, consulte o Capítulo 19, "Referência dos portlets Gerenciamento de Senhas" na página 277.

Para saber mais sobre *administração de portlet*, consulte o Capítulo 9, "Administração de Portlet" na página 179.

Para saber sobre importação e a exportação de dados de portal, consulte o Capítulo 14, "Ferramentas para a exportação e a importação de dados de portal" na página 227.

Para saber mais sobre recursos de *organogramas*, consulte o Capítulo 18, "Referência do portlet Organograma" na página 261.

Para saber mais sobre a função de *pesquisa de diretório*, consulte o Capítulo 20, "Referência do portlet Lista de Pesquisa" na página 291.

Para saber mais sobre opções para a criação de novos objetos (portlet *Criar*) e como eles são administrados, consulte o Capítulo 16, "Criar referência de portlet" na página 241.

Para obter mais informações sobre a configuração e administração de *workflow*, consulte o Capítulo 21, “Introdução ao aprovisionamento com base em workflow” na página 307, bem como o Capítulo 22, “Configurando definições de solicitação de aprovisionamento” na página 321 e o Capítulo 23, “Gerenciando workflows de aprovisionamento” na página 343.

Projetando o ambiente de produção

2

Este capítulo aborda as questões relacionadas à configuração de um ambiente de produção. Ele fornece orientação sobre diversas considerações relevantes durante a transição de um ambiente de teste (ou de pré-produção) para o ambiente de produção.

A organização deste capítulo apresenta as seguintes seções principais:

2.1 Topologia

A quantidade de instâncias de cada subsistema principal e as maneiras como eles podem ser conectados são bastante numerosas. Contudo, nem todos os layouts possíveis têm suporte. É importante compreender não apenas as possibilidades, mas também as razões pelas quais algumas configurações prevalecem sobre outras.

2.1.1 Design mínimo

A configuração lógica mais simples do aplicativo de usuário é a instalação que tem um pouco de tudo e consiste em uma árvore do cofre de identidade, uma instância dos drivers e do mecanismo do Identity Manager e uma instância do JBoss que executa uma instância única do aplicativo de usuário. Em termos de implementação física, teoricamente, você pode executar todos esses componentes em uma configuração. Contudo, há vários motivos (segurança, manutenção e desempenho são os principais) para que você não o faça. Ao escolher o número de computadores necessários para uma instalação real e prática, convém considerar pelo menos o seguinte:

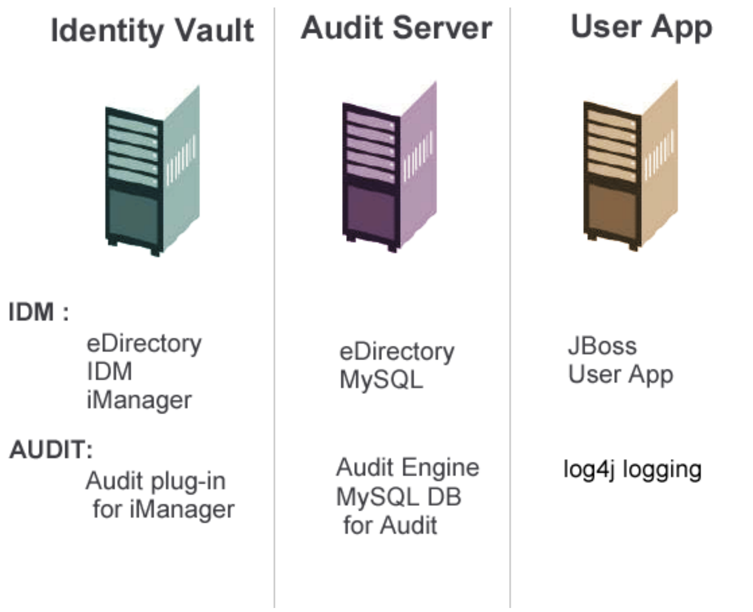
- *Servidor Novell Audit:* esse item é responsável pela captura de informações de evento (e, possivelmente, muitos outros tipos de informações) do ambiente do aplicativo de usuário em tempo de execução. Ele também pode servir como armazenamento persistente para outros aplicativos da empresa. Por diversos motivos, provavelmente você incluirá outros itens importantes do sistema do Identity Manager (por exemplo, JBoss ou o cofre de identidade) na mesma máquina do servidor Audit.
- *Cofre de identidade:* esse é um componente de uso intenso e requer bom desempenho e boa escalabilidade. É bem provável que você considere instalar o cofre de identidade em uma máquina dedicada. Em outras palavras, não convém ter outro sistema de tráfego intenso, como o JBoss com uma distribuição do aplicativo de usuário, sendo executado em conjunto com o cofre de identidade na mesma máquina.
- *Banco de dados:* se essa instância do MySQL (ou outro banco de dados que tenha suporte) também for seu banco de dados do Novell Audit, ela provavelmente estará em uma máquina

dedicada. Lembre-se de que esse item é usado pelo aplicativo de usuário das seguintes maneiras:

- Como armazenamento persistente de dados de configuração do portal
- Como o armazenamento persistente de informações sobre estado de workflows em andamento (se o Módulo de Aprovisionamento estiver instalado)
- Opcionalmente, como o armazenamento de registro do Novell Audit.

- *JBoss:* por questões de desempenho e capacidade, é recomendável executar esse item em uma máquina dedicada.

Essas considerações sugerem a seguinte configuração mínima com três computadores:



2.1.2 Design de alta disponibilidade

O uso de clusters para alta disponibilidade/capacidade será discutido detalhadamente em uma seção posterior deste capítulo. No momento, é importante saber que:

- O Identity Manager permite alta disponibilidade do cofre de identidade, mecanismo e drivers por meio de uma instalação de vários nós e mecanismos de armazenamento compartilhado, descritos no capítulo sobre “Alta disponibilidade” do principal Guia de Administração do Identity Manager. Há instruções detalhadas sobre a configuração de um sistema desse tipo usando o SUSE Linux no artigo em:

  http://support.novell.com/cgi-bin/search/searchtid.cgi?/10093317.htm (http://support.novell.com/cgi-bin/search/searchtid.cgi?/10093317.htm)

- A alta disponibilidade do aplicativo de usuário pode ser obtida por meio dos clusters do JBoss. Você pode configurar um cluster do JBoss de forma que cada nó execute uma instância do aplicativo de usuário. As instâncias estarão no mesmo nível (sem hierarquia). No entanto, não haverá replicação de sessões entre as instâncias. Cada instância será responsável por sua própria unidade de trabalho e não encerrará sessões iniciadas em um nó irmão.

- Pelos motivos já expostos, não há suporte para failover automático. Contudo, um workflow interrompido poderá prosseguir após a perda de um nó do cluster, caso seja colocado online um novo nó com o mesmo ID de mecanismo de workflow. (Nesse caso, o workflow continuará automaticamente assim que o novo mecanismo de workflow for iniciado.)

Consulte a Seção 2.4, "Clusters" na página 47 (mais adiante) para obter informações mais detalhadas sobre essas questões.

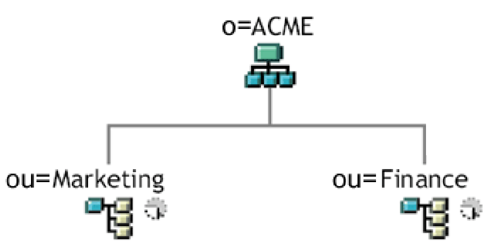
2.1.3 Limitações de design

Em geral, as duas limitações de arquitetura mais importantes que você deve ter em mente são:

- Nenhuma instância de aplicativo de usuário pode atender (pesquisar/consultar, adicionar usuários e assim por diante) a mais de um container de usuário. Além disso, após a associação de um container de usuário ao aplicativo, essa associação é tida como permanente.
- Nenhum Driver de Aplicativo do Usuário pode ser associado a mais de um aplicativo de usuário, exceto quando os aplicativos de usuário estão instalados em nós irmãos no mesmo cluster do JBoss. Em outras palavras, não há suporte ao mapeamento de um driver para muitos aplicativos de usuário.

O primeiro container assegura o uso obrigatório de um alto grau de encapsulação no projeto de aplicativo de usuário.

Suponha que você tenha a seguinte estrutura organizacional:



Durante a instalação do aplicativo de usuário, você é solicitado a especificar o container de usuário de nível superior que sua instalação deverá pesquisar no cofre de identidade. Nesse caso, você poderia especificar *ou=Marketing,o=ACME* ou (como alternativa) *ou=Finance,o=ACME*. Você não poderá especificar ambos. Todas as pesquisas e consultas de aplicativo de usuário (e logins de administrador) terão como escopo o container que você especificou.

Observação: Teoricamente, você poderia especificar o escopo *o=ACME* a fim de englobar Marketing e Finance. Contudo, em organizações grandes com possivelmente muitos containers *ou* (em vez de apenas dois associados a Marketing e Finanças), isso não seria conveniente.

Obviamente, é possível criar duas instalações independentes do aplicativo de usuário (sem recursos em comum), uma para Marketing e outra para Finanças. Cada instalação teria seu próprio banco de dados, bem como seu próprio Driver de Aplicativo do Usuário corretamente configurado, e cada aplicativo de usuário seria administrado separadamente e, se possível, teria um tema exclusivo.

Caso seja absolutamente necessária a instalação dos containers Marketing e Finance no mesmo escopo em uma instalação do aplicativo de usuário, há duas possíveis estratégias a serem consideradas. Uma delas é inserir um novo objeto container (por exemplo,

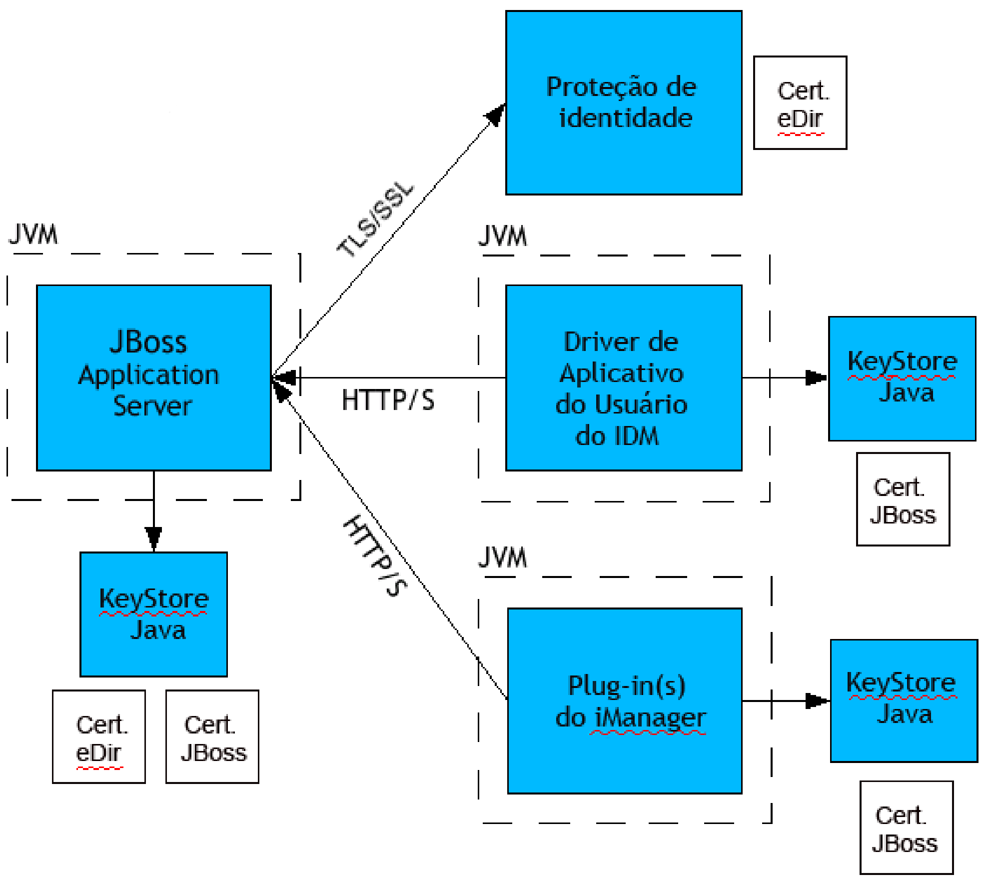
ou=MarketingAndFinance) na hierarquia, acima dos dois nós irmãos e, em seguida, apontar para o novo container como a raiz do escopo. A outra estratégia é criar uma réplica filtrada (um tipo especial de árvore do eDirectory) que combine as partes necessárias da árvore ACME, e apontar o aplicativo de usuário em direção ao container raiz da réplica. (Consulte o eDirectory Administration Guide (Guia de Administração do eDirectory) para obter mais informações sobre réplicas filtradas.)

Se tiver dúvidas sobre um layout de sistema em particular, entre em contato com seu representante da Novell para obter assistência ou orientação.

2.2 Segurança

Passar da pré-produção à produção em geral envolve o fortalecimento dos aspectos de segurança do sistema. É possível que você tenha usado o protocolo HTTP normal em seu ambiente de teste para conectar o driver do aplicativo de usuário ao JBoss, ou então, tenha usado um certificado com auto-assinatura (como medida temporária) na comunicação driver/servidor de aplicativos. Por outro lado, é provável que, no ambiente de produção, você utilize conexões seguras, com autenticação de servidor baseada no certificado da Verisign (ou de outro provedor confiável) de sua empresa.

Tipicamente, os certificados X.509 podem ser usados em diversos lugares no ambiente do aplicativo de usuário do Identity Manager, conforme mostra o diagrama a seguir.



As comunicações entre o aplicativo de usuário e o cofre de identidade são protegidos por padrão usando TLS (Transport Layer Security). A instalação do certificado do cofre de identidade (eDirectory) no keystore do JBoss é feita automaticamente no momento da instalação. A menos que

você especifique o contrário, o instalador do aplicativo de usuário coloca uma cópia do certificado do eDirectory no armazenamento *cacerts* padrão do JRE.

O certificado do servidor precisa estar em diversos locais para que as comunicações sejam seguras, como mostra o diagrama. Diversas etapas de configuração podem ser necessárias se você pretende usar um certificado auto-assinado nos vários locais indicados no diagrama por uma caixa *JBoss cert* ou se prefere usar um certificado emitido por uma AC (autoridade de certificação) confiável como a Verisign.

Certificados auto-assinados

Se você utiliza um certificado de um emissor conhecido e confiável (por exemplo, a Verisign), não são necessárias etapas especiais de configuração. Porém, se você pretende criar e usar um certificado auto-assinado, precisa seguir estas etapas:

1. Crie um keystore com um certificado auto-assinado usando uma sintaxe de linha de comando semelhante a esta:

   ```
   keytool -genkey -alias tomcat -keyalg RSA -storepass changeit -
   keystore jboss.jks -dname
   "cn=JBoss,ou=exteNd,o=Novell,l=Waltham,s=MA,c=US" -keypass
   changeit
   ```

   Lembre-se de que você está criando o arquivo “jboss.jks”, bem como o certificado.
2. Copie o arquivo de keystore (jboss.jks) para o diretório do aplicativo de usuário do JBoss, por exemplo:

   ```
   cp jboss.jks ~/jboss-4.0.2/server/spitfire/conf
   ```

Ativando o SSL no JBoss

Para habilitar o SSL no JBoss, localize o arquivo *jbossweb-tomcat55.sar* em *[IDM]/jboss/server/IDM/deploy/.* Procure o arquivo *server.xml* e abra-o em um editor de texto. Para habilitar o SSL, retire o comentário ou adicione uma seção parecida com esta:

```
<Connector port="8443" address="${jboss.bind.address}"
maxThreads="100" strategy="ms" maxHttpHeaderSize="8192"
emptySessionPath="true" scheme="https" secure="true"
clientAuth="false" keystoreFile="${jboss.server.home.dir}/spitfire/
conf/jboss.jks" keystorePass="changeit" sslProtocol = "TLS" />
```

Ativando a segurança SOAP

Em *IDM.war*, procure o arquivo *web.xml* e abra-o em um editor de texto. Na parte inferior do arquivo, retire o comentário da seguinte seção:

```
<security-constraint> <web-resource-collection> <web-resource-
name>IDMProv</web-resource-name> <url-pattern>/*</url-pattern> <http-
method>POST</http-method> <http-method>GET</http-method>
<description>IDM Provisioning Edition</description> </web-resource-
```

```
collection> <user-data-constraint> <transport-guarantee>CONFIDENTIAL</
transport guarantee> </user-data-constraint> </security-constraint>
```

Grave o arquivo e o arquivamento. Reinicie o Jboss.

2.2.1 Autenticação mútua

O aplicativo de usuário do Identity Manager oferece suporte a cenários tradicionais de *autenticação de servidor* (normalmente usada em sessões https com *páginas da Web seguras* na Web), mas não oferece suporte imediato à autenticação de certificado bidirecional. Contudo, essa função pode ser obtida com o Novell iChain. Portanto, por exemplo, se em sua organização for necessário que os usuários efetuem login com um certificado de usuário, e não com uma senha, isso será possível se você adicionar o iChain ao ambiente.

Para obter mais informações, consulte o representante da Novell.

2.3 Ajuste do desempenho

O ajuste do desempenho é um assunto complexo. O aplicativo de usuário do Identity Manager depende de diversas tecnologias com várias interações. Não é possível prever todos os cenários de configuração ou de interação do usuário que podem prejudicar o desempenho. Porém, alguns subsistemas estão sujeitos a melhores práticas que incrementam o desempenho. Esse assunto será discutido a seguir.

2.3.1 Registro

O aplicativo de usuário permite o registro por meio do Novell Audit e também da estrutura de código-fonte aberto *log4j* da Apache. Por padrão, o registro por meio do Novell Audit é desabilitado. Contudo, o registro no arquivo e no console através de *log4j* é habilitado por padrão.

Observação: Os tipos de eventos que você pode registrar e a maneira de habilitar ou desabilitar o registro serão abordados no Capítulo 5, “Configurando o registro” na página 119 e no Capítulo 12, “Configuração de Registro” na página 211, mais adiante neste guia.

As definições de configuração de *log4j* estão contidas em um arquivo denominado *log4j.xml*, em *$IDMINSTALL/jboss/server/IDMProv/conf/*. Quase no final desse arquivo, você encontrará a seguinte entrada:

```
<root>     <priority value="INFO" />     <appender-ref ref="CONSOLE" /
>     <appender-ref ref="FILE" /> </root>
```

A atribuição de um valor a `root` garante que qualquer appender de registro que não tenha um nível explicitamente atribuído herde o nível `root` (nesse caso, INFO). Por exemplo, por padrão, não há um nível de limite atribuído ao appender FILE; portanto, ele assume o nível da raiz (root).

Os níveis de registro possíveis usados por *log4j* são DEBUG, INFO, WARN, ERROR e FATAL, conforme definido na classe *org.apache.log4j.Level*. O desempenho poderá ser prejudicado caso essas configurações não sejam utilizadas apropriadamente.

Uma regra útil a seguir é utilizar INFO ou DEBUG apenas ao depurar um problema específico.

Qualquer appender incluído na raiz cujo limite de nível não tenha sido definido deverá ter esse limite especificado como ERROR, WARN ou FATAL, a menos que você esteja depurando algo (como explicado acima).

O desempenho é afetado devido ao alto nível de registro; isso não é decorrente das mensagens verbosas, mas ao fato de que o registro de console e de arquivo em *log4j* envolve gravações síncronas. Uma classe `AsyncAppender` está disponível, mas seu uso não garante um melhor desempenho. Os problemas (os quais são conhecidos, sendo problemas do *log4j* da Apache, e não do Identity Manager) estão documentados em *http://logging.apache.org/log4j/docs/api-1.2.8/org/apache/log4j/performance/Logging.html*.

O padrão INFO no arquivo de configuração de registro do aplicativo de usuário (acima) é adequado em vários ambientes, mas quando o desempenho for crucial, você deverá considerar a mudança da entrada *log4j.xml* acima para:

```
<root> <priority value="ERROR"/> <appender-ref ref="FILE"/> </root>
```

Em outras palavras, remova CONSOLE e defina o nível do registro como ERROR. Para obter uma configuração de produção totalmente testada/depurada, não é necessário definir o registro no nível INFO, nem deixar o modo de registro CONSOLE habilitado. O ganho em desempenho ao desativá-los pode ser significativo.

Para obter mais informações sobre o *log4j*, consulte a documentação disponível em *http://logging.apache.org/log4j/docs*.

Para obter mais informações sobre o uso do Novell Audit com o Identity Manager, consulte o Guia de Administração do Novell Identity Manager.

2.3.2 Cofre de identidade

Consultas LDAP podem causar gargalos em um ambiente de servidor-diretório de uso intenso. Para manter um alto nível de desempenho quando há grande quantidade de objetos, o Novell eDirectory (que forma a base do cofre de identidade no Identity Manager) registra informações solicitadas com freqüência e as armazena em índices. Quando uma consulta complexa é feita em relação a objetos com atributos indexados, o resultado da consulta é obtido de forma muito mais rápida.

O eDirectory é fornecido com os seguintes atributos já indexados:

```
Nome do Objeto que Originou o Álias cn dc Equivalente a mim
extensionInfo Nome GUID ldapAttributeList ldapClassList Member NLS:
Common Certificate Obituário Referência Revisão Sobrenome uniqueID
uniqueID_SS
```

Quando você instala o Identity Manager, o esquema de diretório padrão é estendido com novos tipos de objectclass e novos atributos pertinentes ao aplicativo de usuário. Por padrão, os atributos específicos ao aplicativo de usuário não são indexados. Para a obtenção do melhor desempenho, pode ser útil indexar alguns desses atributos (e talvez também alguns atributos LDAP tradicionais), sobretudo quando o container de usuário contiver mais de 5 mil objetos.

A idéia geral é indexar apenas os atributos que você já sabe que serão consultados com freqüência. (Os atributos podem ser diferentes em ambientes de produção diversos.) O único modo de determinar com certeza que atributos serão usados com freqüência é coletar estatísticas de atributo em tempo de execução. (No entanto, esse processo de coleta pode prejudicar o desempenho.)

O processo de coleta de estatísticas de atributo é abordado em detalhes no eDirectory Administration Guide (Guia de Administração do eDirectory). A indexação também é abordada em detalhes naquele guia. Em geral, você deverá proceder da seguinte forma:

- Use o Console One para ativar a coleta de estatísticas dos atributos desejados
- Coloque o sistema em funcionamento
- Desabilite a coleta de estatísticas e analise os resultados
- Crie um índice para cada tipo de atributo que possa se beneficiar disso

Se você já sabe que atributos deseja indexar, não precisa usar o Console One. É possível criar e gerenciar índices no iManager por meio de Manutenção > Índices do eDirectory. Por exemplo, se você sabe que os usuários de seu organograma provavelmente realizarão pesquisas com base no atributo *isManager*, poderá tentar indexar esse atributo para determinar se isso melhora o desempenho.

Observação: Como melhor prática, é recomendável indexar, no mínimo, os atributos *gerente* e *isManager*.

Para obter uma descrição detalhada da indexação de atributos e desempenho, consulte o capítulo “Tuning eDirectory” (Ajustando o eDirectory) no manual *Novell’s Guide to Troubleshooting eDirectory* (Guia da Novell para Solução de Problemas do eDirectory) de Peter Kuo e Jim Henderson (QUE Books, ISBN 0-7897-3146-0).

Além disso, consulte o capítulo sobre manutenção do Novell eDirectory (que apresenta instruções sobre o ajuste do desempenho) no *eDirectory Administration Guide* (Guia de Administração do eDirectory) principal.

2.3.3 JVM

A quantidade de memória de pilha alocada para a máquina virtual Java pode prejudicar o desempenho. Se você especificar valores mínimos ou máximos de memória que sejam muito baixos ou muito altos (valores muito altos são os que excedem a memória física do computador), poderá haver um excesso de troca de arquivo de paginação.

Você pode definir o tamanho máximo da JVM do servidor JBoss editando o arquivo `run.conf` ou `run.bat` (o primeiro para Linux, o segundo para Windows) em `[IDM]/jboss/bin/` em um editor de texto. Aumente “-Xmx” de *128m* para *512m*, ou mais, se possível. Pode ser necessário experimentar diferentes configurações para determinar o valor ideal para seu ambiente.

Observação: Há dicas sobre o ajuste do desempenho do JBoss e Tomcat em http://wiki.jboss.org/wiki/Wiki.jsp?page=JBossASTuningSliming (http://wiki.jboss.org/wiki/Wiki.jsp?page=JBossASTuningSliming)

2.3.4 Valor de tempo de espera da sessão

O tempo de espera da sessão (o período em que um usuário pode ficar sem interagir com a página em seu browser da Web antes da exibição de uma caixa de diálogo de aviso de tempo de espera da sessão) pode ser mudado no arquivo *web.xml* presente no arquivo *IDM.war*. Esse valor deve ser ajustado para corresponder ao ambiente de uso e servidor em que o aplicativo será executado. Em geral, é recomendável que o tempo limite da sessão seja o mais curto possível. Caso os requisitos comerciais possam acomodar um tempo limite de sessão de cinco minutos, isso permitirá que o servidor libere recursos não utilizados duas vezes mais rápido do que ao ser usado um valor de tempo limite de 10 minutos. Assim, o aplicativo Web apresentará melhor desempenho e escalabilidade.

Considere o seguinte ao ajustar o tempo limite da sessão:

- Um tempo limite de sessão longo pode fazer com que o servidor JBoss fique sem memória, caso muitos usuários efetuem login em um período de tempo curto. Isso pode acontecer com qualquer servidor de aplicativos com muitas sessões simultâneas em andamento.
- Quando um usuário efetua login no aplicativo de usuário, uma conexão LDAP é criada para esse usuário e vinculada à sessão. Assim, quanto mais sessões estiverem em andamento, maior será o número de conexões LDAP utilizadas. Quanto mais longo o tempo de espera de sessão, maior o tempo durante o qual essas conexões ficam abertas. Um grande número de conexões ao servidor LDAP (mesmo que inativas) pode prejudicar o desempenho do sistema.
- Se o servidor começar a apresentar erros de memória insuficiente, e se os parâmetros de ajuste da coleta de lixo e pilha da JVM já tiverem os melhores ajustes para os ambientes de uso e servidor, convém considerar a redução do tempo limite de sessão.

Para ajustar o valor de tempo limite da sessão, você deverá abrir o arquivamento *IDM.war* , localizar o arquivo *web.xml* nele contido e editar a seguinte seção do arquivo (principalmente o valor numérico, aqui mostrado como 20, que significa 20 minutos, o padrão):

```
<session-config>     <session-timeout>20</session-timeout> </session-
config>
```

Em seguida, grave o arquivo e o arquivamento e reinicie o servidor.

Observação: A edição manual de arquivos em arquivamentos Web deverá ser feita por uma pessoa com experiência em desenvolvimento e distribuição de aplicativos Web Java.

2.4 Clusters

Há três aspectos que você deverá considerar ao usar o aplicativo de usuário em um ambiente em cluster:

- A configuração em cluster do JBoss (consulte a Seção 2.4.1, “Clusters JBoss” na página 48)
- A configuração de cache do aplicativo de usuário (consulte a Seção 2.4.3, “Definindo a configuração de cache do grupo de clusters do aplicativo de usuário” na página 52)
- A configuração do mecanismo de workflow (consulte a Seção 2.4.4, “Configurando workflows para clusters” na página 53)

2.4.1 Clusters JBoss

Um cluster é um conjunto de nós de servidores de aplicativos que fornecem determinados serviços. O propósito de um cluster é aumentar o desempenho e a confiabilidade dos aplicativos. Em geral, um cluster fornece três benefícios principais aos aplicativos empresariais:

- Alta disponibilidade
- Escalabilidade (maior capacidade)
- Equilíbrio de carga

Alta disponibilidade significa que um aplicativo é confiável e está disponível durante grande parte do tempo em que está distribuído. Clusters proporcionam alta disponibilidade, uma vez que o mesmo aplicativo é executado em todos os nós. Caso um nó falhe, o aplicativo ainda será executado em outros nós. O aplicativo de usuário do Identity Manager usufrui de maior disponibilidade ao ser executado em um ambiente em cluster. Contudo, o aplicativo de usuário do Identity Manager não tem suporte para a replicação de sessão http. Isso significa que, se a sessão estiver em andamento em um nó, e esse nó falhar, as informações da sessão serão perdidas.

O equilíbrio de carga é a pratica de distribuir a carga de trabalho entre os membros de um cluster. O objetivo do equilíbrio de carga é aprimorar o desempenho. O equilíbrio de carga pode ser realizado de várias formas (por exemplo, com o rodízio de DNS ou equilíbrio de carga de hardware). Consulte http://www.onjava.com/pub/a/onjava/2001/09/26/load.html (http://www.onjava.com/pub/a/onjava/2001/09/26/load.html) para obter uma abordagem dos diversos métodos de equilíbrio de carga. Seja qual for o método selecionado, convém incluir o equilíbrio de carga em sua configuração de cluster.

Grupos de clusters JBoss

Os clusters JBoss são baseados em um módulo de comunicação chamado JGroups. O JGroups é instalado com o JBoss (ele também pode ser usado sem o JBoss). Os JGroups proporcionam a comunicação entre grupos, que compartilham um nome, um endereço de multicast e uma porta de multicast comuns.

Quando você instala um servidor JBoss em cluster, o JBoss define dois grupos JGroups diferentes para o uso no gerenciamento do cluster. Um é chamado *DefaultPartition* e é definido em /deploy/cluster-service.xml. Esse grupo de clusters é usado pelo JBoss para fornecer serviços de cluster básicos. O JBoss também define um segundo grupo de clusters chamado *Tomcat-Cluster*. Esse grupo de clusters é definido em /deploy/tc-cluster-service.xml. Esse grupo de clusters fornece a replicação de sessão para o servidor Tomcat executado no JBoss.

O aplicativo de usuário do Identity Manager usa um terceiro grupo de clusters. Esse grupo de clusters usa um nome UUID para minimizar o risco de conflitos com outros grupos de clusters que os usuários possam adicionar a seus servidores. Por padrão, o grupo de clusters é chamado `c373e901aba5e8ee9966444553544200`. Esse cluster não é configurado usando um arquivo de serviço JBoss. Em vez disso, as configurações estão localizadas no diretório e podem ser definidas usando os recursos de administração do aplicativo de usuário. Se estiver familiarizado com clusters JGroups e JBoss, você poderá ajustar as configurações de cluster do aplicativo de usuário por meio dessa interface. Mudanças na configuração de cluster entram em vigor em um nó de servidor somente após ele ter sido reiniciado.

O grupo de clusters do aplicativo de usuário é usado apenas para coordenar os caches do aplicativo de usuário em um ambiente em cluster. Ele não depende dos dois grupos de clusters JBoss, nem interage com eles de modo algum. Por padrão, o grupo de clusters de aplicativo de usuário e os dois

grupos JBoss usam nomes de grupo, endereços e portas de multicast diferentes, assim, não é necessária a reconfiguração.

As configurações do grupo de clusters do aplicativo de usuário são compartilhadas por qualquer aplicativo do Identity Manager 3 que compartilhe a mesma configuração de diretório. O propósito da opção de configurações locais na interface de administração do aplicativo de usuário é permitir que um administrador remova um nó de um cluster, ou mude a participação de servidores em um cluster. Por exemplo, você pode desabilitar o uso global de cluster e, em seguida, habilitá-lo localmente para um subconjunto de servidores que compartilhem a configuração de diretório.

Farm de Aplicativos

O JBoss permite a distribuição do tipo "hot-deploy" em um cluster copiando um aplicativo EAR, WAR ou JAR para o diretório da farm de uma instância do JBoss em cluster. A distribuição “hot” em um computador faz com que o componente seja distribuído automaticamente a todas as instâncias no cluster durante a sua execução.

Esse modo de distribuição de aplicativo não é recomendado com a versão do JBoss Application Server (4.0.2) incluída com o programa de instalação do aplicativo de usuário durante a criação deste documento, pois há problemas relacionados ao seu uso que ainda não foram resolvidos. No entanto, fornecemos as etapas básicas que devem ser realizadas (consulte “Distribuindo o aplicativo de usuário em um cluster usando farming do JBoss” na página 52) para a distribuição bem-sucedida do aplicativo de usuário utilizando a tecnologia de farming do JBoss, já que é provável que essa tecnologia seja aprimorada após a publicação deste documento.

Banco de dados MySQL

O programa de instalação do aplicativo de usuário pode instalar o gerenciador de banco de dados MySQL e criar um banco de dados para uso com o aplicativo de usuário, ou então pode utilizar um banco de dados Oracle, Microsoft SQL Server ou MySQL. O banco de dados é responsável pela persistência de dados. Todos os nós no cluster JBoss devem acessar a mesma instância de banco de dados. O aplicativo de usuário utiliza chamadas JDBC padrão para acessar e atualizar o banco de dados. O aplicativo de usuário utiliza uma fonte de dados JDBC vinculada à árvore JNDI para abrir uma conexão ao banco de dados. Se você criar um cluster JBoss usando o programa de instalação do aplicativo de usuário, a fonte de dados será instalada automaticamente. Se você optar por instalar manualmente o cluster JBoss, deverá copiar o arquivo de fonte de dados (IDM-ds.xml) no diretório de distribuição em todos os nós do cluster. Além disso, se estiver usando o MySQL, você deverá copiar o driver JDBC do MySQL (*mysql-connector-java-3.1.10-utf8-clob-fix-bin.jar*), localizado no diretório /server/IDM/lib do JBoss, no diretório server/IDM/lib do JBoss.

Registro

Para habilitar o registro em clusters, você deverá editar o arquivo de configuração log4j.xml, localizado no diretório \conf da configuração do servidor JBoss (por exemplo, \server\IDM\conf), e retirar as marcas de comentário da seção na parte inferior similar a:

```
<!-- Registro de clusters --> - <!-- Retire a marca de comentário do
código a seguir para redirecionar as categorias org.jgroups e
org.jboss.ha a um arquivo cluster.log. <appender name="CLUSTER"
class="org.jboss.logging.appender.RollingFileAppender"> <errorHandler
class="org.jboss.logging.util.OnlyOnceErrorHandler"/> <param
name="File" value="${jboss.server.home.dir}/log cluster.log"/> <param
name="Append" value="false"/> <param name="MaxFileSize" value="500KB"/
```

```
> <param name="MaxBackupIndex" value="1"/> <layout
class="org.apache.log4j.PatternLayout"> <param
name="ConversionPattern" value="%d %-5p [%c] %m%n"/> </layout> </
appender> <category name="org.jgroups"> <priority value="DEBUG" />
<appender-ref ref="CLUSTER"/> </category> <category
name="org.jboss.ha"> <priority value="DEBUG" /> <appender-ref
ref="CLUSTER"/> </category> -->
```

O arquivo *cluster.log* está no diretório *log* da configuração do servidor JBoss (por exemplo, *\server\IDM\log*).

2.4.2 Instalando o aplicativo de usuário em um cluster JBoss

O método recomendado de instalação do aplicativo de usuário em um cluster é o uso do programa de instalação do aplicativo de usuário para instalá-lo em cada nó do cluster. Embora não recomendemos a distribuição do aplicativo de usuário em um cluster usando o método de farming do JBoss, incluímos um procedimento que pode ser executado como método alternativo.

Usando o programa de instalação do aplicativo de usuário em cada nó do cluster

O JBoss é fornecido com três configurações de servidor prontas para o uso: *mínima*, *padrão* e *todos*. Clusters são habilitados apenas na configuração *todos*. O arquivo cluster-service.xml na pasta /deploy descreve a configuração da partição de cluster padrão. Quando você instala o aplicativo de usuário e indica ao programa de instalação que deseja instalá-lo em um cluster, o programa de instalação faz uma cópia da configuração *todos*, nomeia a cópia *IDM* (por padrão, o programa de instalação permite mudar o nome) e instala o aplicativo de usuário nessa configuração.

Para instalar o aplicativo de usuário em cada nó do cluster usando o programa de instalação do aplicativo de usuário:

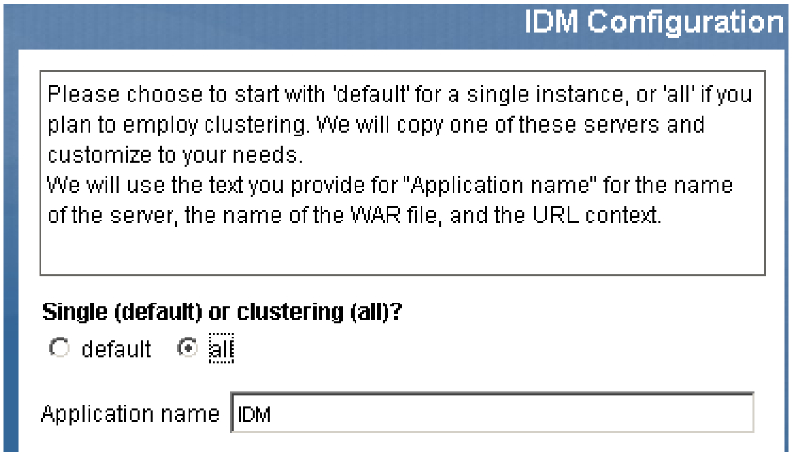
1. Execute uma instalação completa do aplicativo de usuário (MySQL, JBoss e o aplicativo de usuário) no primeiro nó JBoss. Para obter informações sobre o uso do programa de instalação do aplicativo de usuário, consulte o *Guia de Instalação do Identity Manager 3*.
   - Se você estiver usando MySQL como o banco de dados do aplicativo de usuário, o instalador do aplicativo de usuário criará uma nova instalação do MySQL. Anote a senha de usuário raiz do MySQL que especificar; você precisará dessa informação ao instalar o aplicativo de usuário nos outros nós do cluster.
   - Na tela *Configuração do IDM* do programa de instalação, selecione a opção "*cluster (tudo)*".
   - Selecione outras opções de instalação conforme apropriado em seu ambiente.
2. Se o MySQL não estiver em execução, inicie-o usando o arquivo *start-mysql.bat* no diretório /IDM/mysql.

   Observação: No Linux, o seguinte comando shell será útil para determinar se o daemon MySQL está em execução:

   ```
   ps -A | grep mysqld
   ```

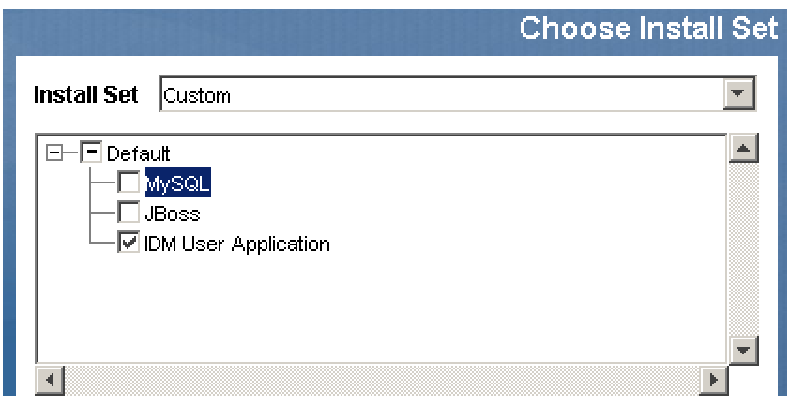
Se esse comando resultar em várias linhas terminadas em `mysqld`, isso significa que o daemon está em execução.

3 Inicie o JBoss e o aplicativo de usuário utilizando o arquivo *start-jboss.bat* (Windows) ou *start-jboss.sh* (Linux), localizado no diretório *IDM*.



4 Execute uma instalação personalizada do aplicativo de usuário em cada nó adicional do cluster JBoss.

- Selecione apenas o aplicativo de usuário para instalação:



- Especifique o endereço IP ou nome de host do servidor no qual o banco de dados do aplicativo de usuário está instalado.
- Especifique o nome de usuário e a senha do banco de dados do aplicativo de usuário. Se você estiver usando MySQL, o nome de usuário é `root`, e a senha é aquela especificada durante o processo de instalação em Etapa 1.
- Na tela *IDM Configuration* do programa de instalação, selecione a opção "*cluster (tudo)*".
- Selecione outras opções de instalação conforme apropriado em seu ambiente.

5 Inicie cada nó do cluster JBoss utilizando o arquivo *start-jboss.bat* (Windows) ou *start-jboss.sh* (Linux), localizado no diretório *IDM*.

Distribuindo o aplicativo de usuário em um cluster usando farming do JBoss

Não use o recurso de farming do JBoss com a versão 4.0.2 ou anterior, pois poderá encontrar problemas (consulte http://jira.jboss.com/jira/browse/JBAS-1899 (http://jira.jboss.com/jira/browse/JBAS-1899)). Recomendamos a instalação do aplicativo de usuário em cada nó do cluster por meio do programa de instalação do aplicativo de usuário (consulte "Usando o programa de instalação do aplicativo de usuário em cada nó do cluster" na página 50 neste Capítulo). Contudo, se desejar usar farming para distribuir o aplicativo de usuário em um cluster JBoss usando o JBoss 4.0.3 ou posterior, siga as etapas abaixo.

Observação: Essas etapas destinam-se a clientes que desejam usar o JBoss 4.0.3 por conta própria para experimentar essa configuração. A versão oficialmente suportada é a 4.0.2.

Para distribuir o aplicativo de usuário em um cluster usando farming do JBoss:

1. Execute uma instalação personalizada do aplicativo de usuário em um dos nós do cluster JBoss, selecionando o aplicativo de usuário e o MySQL (se estiver usando MySQL; do contrário, instale apenas o aplicativo de usuário) para a instalação. Você pode realizar a instalação com todos os clusters executados no nó, porém, o nó para a instalação do aplicativo de usuário deverá ser o primeiro nó no cluster a ser iniciado.
2. Copie o arquivo de driver JDBC (por exemplo, se estiver usando o MySQL, o driver JDBC estará em *mysql-connector-java-3.1.10-utf8-clob-fix-bin.jar*), localizado no diretório /server/IDM/lib, no diretório correspondente em cada nó do cluster.
3. Copie o arquivo *cacerts* do diretório /lib/security do JRE instalado com o aplicativo de usuário no diretório /lib/security do JRE de cada nó do cluster.
4. Mova o arquivo IDM.war e o arquivo de fonte de dados IDM-ds.xml do diretório /deploy, no diretório de configuração do servidor, para o diretório /farm no diretório de configuração do servidor. Você deve mover de fato os arquivos. Não deixe os originais no diretório /deploy.
5. Inicie o banco de dados do aplicativo de usuário (se estiver usando o MySQL fornecido, inicie-o utilizando o arquivo *start-mysql.bat* localizado no diretório /IDM/mysql).
6. Inicie o JBoss e o aplicativo de usuário utilizando o arquivo *start-jboss.bat* (Windows) ou *start-jboss.sh* (Linux), localizado no diretório *IDM* no nó em que instalou o aplicativo de usuário e o banco de dados do aplicativo de usuário.
7. Inicie os outros nós no cluster.

2.4.3 Definindo a configuração de cache do grupo de clusters do aplicativo de usuário

Usuários familiarizados com clusters JGroups e JBoss podem modificar as configurações de cache do grupo de clusters usando a interface de administração do aplicativo de usuário (consulte a Seção 13.3.5, "Configurações de cache para clusters" na página 224). Mudanças na configuração de cluster entram em vigor em um nó de servidor somente após esse nó ter sido reiniciado.

2.4.4 Configurando workflows para clusters

O mecanismo de workflow em cluster funciona de modo independente da estrutura de cache do aplicativo de usuário. Há diversas etapas a serem executadas para garantir que o mecanismo de workflow funcione corretamente em um ambiente de cluster.

- Todos os servidores no cluster devem estar apontando para o mesmo banco de dados. Se você instalar o aplicativo de usuário no cluster usando o método recomendado (consulte "Usando o programa de instalação do aplicativo de usuário em cada nó do cluster" na página 50), poderá fazer isso durante o processo de instalação especificando o endereço IP ou nome de host do servidor no qual o banco de dados do aplicativo de usuário está instalado. Se você usar o método de farming para distribuir o aplicativo de usuário a nós do cluster (consulte "Distribuindo o aplicativo de usuário em um cluster usando farming do JBoss" na página 52), poderá fazer isso movendo o arquivo de fonte de dados (IDM-ds.xml) do diretório /deploy ao diretório /farm no nó em que o aplicativo de usuário está instalado. Isso faz com que a fonte de dados seja distribuída em todos os nós do cluster.
- Cada servidor no cluster deverá ser iniciado com um ID de mecanismo exclusiva. Isso pode ser feito configurando a propriedade de sistema *com.novell.afw.wf.engine-id* na inicialização do servidor. Por exemplo, se desejar iniciar o JBoss e atribuir o ID de mecanismo `ENGINE1` ao mecanismo de workflow do servidor, você poderá usar o seguinte comando:

  run.sh -Dcom.novell.afw.wf.engine-id=ENGINE1 (Linux)

  run.bat -Dcom.novell.afw.wf.engine-id=ENGINE1 (Windows)

Após ser iniciada por um mecanismo de workflow executado em um determinado servidor, a instância do processo de workflow poderá ser executada e concluída apenas naquele servidor. Isso garante a execução segura do processo do workflow. Contudo, não fornece suporte de failover à instância do processo. Se um servidor em um cluster falhar, a instância do processo só será reiniciada quando um mecanismo com o mesmo ID for reiniciado.

Se um servidor não puder ser reiniciado devido a uma falha grave de hardware ou software, você poderá iniciar o servidor do aplicativo em um novo computador usando o mesmo ID de mecanismo de workflow usado no computador que não pôde ser recuperado. Como o ID de mecanismo é um nome lógico, e não um mapeamento direto ao computador físico no qual o mecanismo era executado, a instância do processo interrompida será concluída com êxito no novo computador.

Instâncias de processo pertencem ao mecanismo que iniciou o processo. Contudo, um usuário pode efetuar login em qualquer aplicativo de usuário em um cluster para ver detalhes do processo, recolher processos ou concluir tarefas a ele atribuídas. Processos que são recolhidos ou tarefas concluídas em um mecanismo ao qual o processo não pertence registram um estado de pendente e recomeçam sua execução após serem descobertos pelo mecanismo ao qual pertencem.

Configurando o ambiente do aplicativo de usuário

II

Estes capítulos descrevem como configurar os vários aspectos do ambiente do aplicativo de usuário do Identity Manager para atender às necessidades de sua organização.

Configurando o Driver de Aplicativo do Usuário

3

3.1 Sobre o Driver de Aplicativo do Usuário

O driver de aplicativo do usuário é responsável por iniciar os workflows de aprovisionamento e notificar o aplicativo de usuário sobre mudanças no Cofre de Identidade (por exemplo, quando você faz mudanças na camada de abstração de diretório usando o Designer do Identity Manager). Apenas o canal do Assinante é usado nesse driver. O driver processa as mensagens do Cofre de Identidade ao aplicativo de usuário executado no servidor de aplicativos. Embora haja eventos que ocorrem no aplicativo de usuário e são relatados ao Cofre de Identidade, esses eventos não fluem através do canal Editor do driver de aplicativo de usuário.

Quando o servidor de aplicativos é iniciado, o driver estabelece com ele uma sessão. O driver envia mensagens ao aplicativo de usuário executado no servidor de aplicativos (por exemplo, "recuperar um novo conjunto de definições de diretório virtual"

Os componentes de origem do driver incluem:

- ComposerDriverShim.jar – o shim do driver do Composer. É instalado no diretório *lib \Novell\NDS\lib* no Windows ou no diretório *classes* (*/usr/lib/dirxml/classes*) no Linux
- srvprvUAD.jar – O shim do driver de aplicativo É instalado no diretório *lib \Novell\NDS\lib* no Windows ou no diretório *classes* (*/usr/lib/dirxml/classes*) no Linux
- UserApplicationDriver.xml – um arquivo que contém dados de pré-configuração para definir o novo driver. É instalado no diretório *DirXML.Drivers* (*\Tomcat\webapps\nps\DirXML.Drivers*) no Windows ou */usr/lib/dirxml/rules/DirXML.Drivers* no Linux

Os componentes do driver de aplicativo do usuário são instalados quando você instala o Identity Manager 3. Para poder executar o aplicativo de usuário do Identity Manager 3, adicione o driver de aplicativo do usuário a um conjunto de drivers novo ou existente e ative o driver.

Dependendo de seu ambiente de trabalho, será necessária pouca configuração do driver de aplicativo do usuário, ou você poderá implementar um conjunto complexo de regras comerciais nas políticas de driver. O driver de aplicativo do usuário fornece os mesmos mecanismos flexíveis para sincronização de dados que outros drivers do Identity Manager.

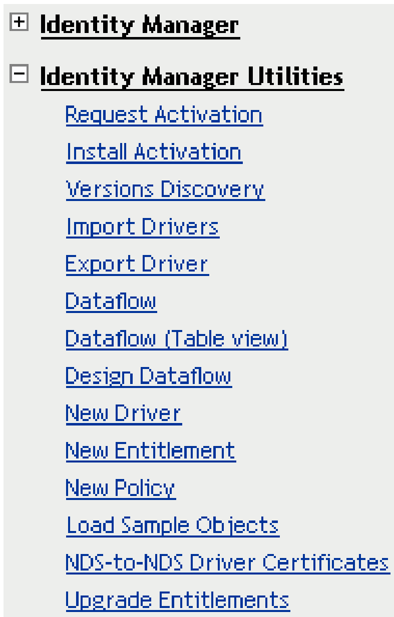
Este Capítulo descreve como criar, configurar e iniciar um driver de aplicativo do usuário e como configurar o driver para acionar um workflow automaticamente em resposta a um evento no Cofre de Identidade. Ele contém as seguintes seções:

3.2 Criando o Driver de Aplicativo do Usuário

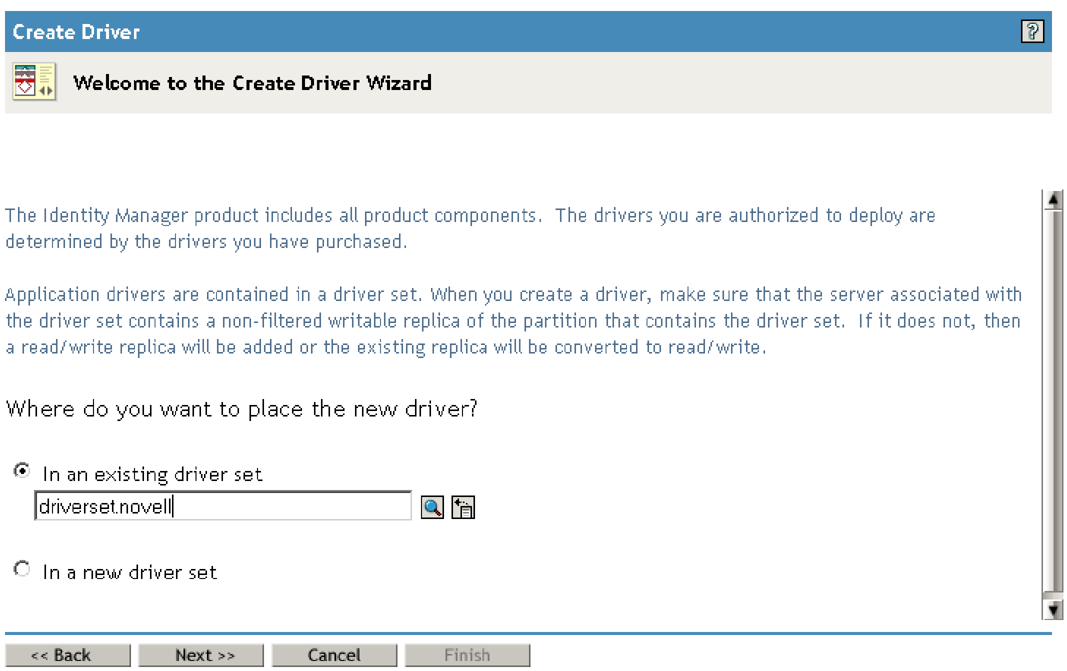
Para criar o driver:

1 Efetue login na instância do iManager que gerencia seu Cofre de Identidade.

2 Abra o nó *Utilitários do Identity Manager* no frame de navegação do iManager.



3 Clique em *Novo Driver*. O Assistente de Criação de Driver é exibido:

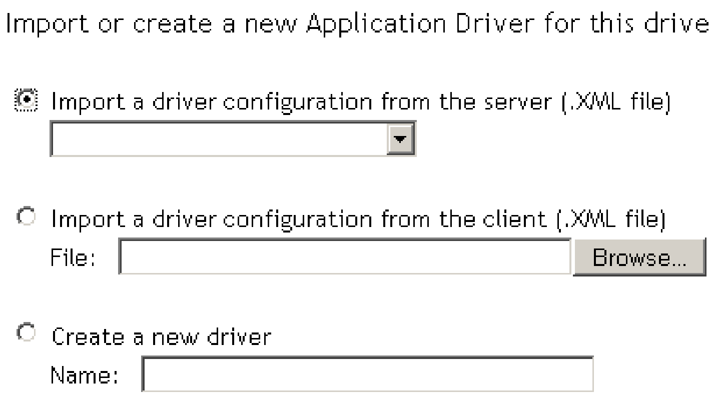


A próxima etapa é selecionar onde criar o novo driver. Você pode criar o driver em um conjunto de drivers existente ou criar um novo conjunto de drivers.

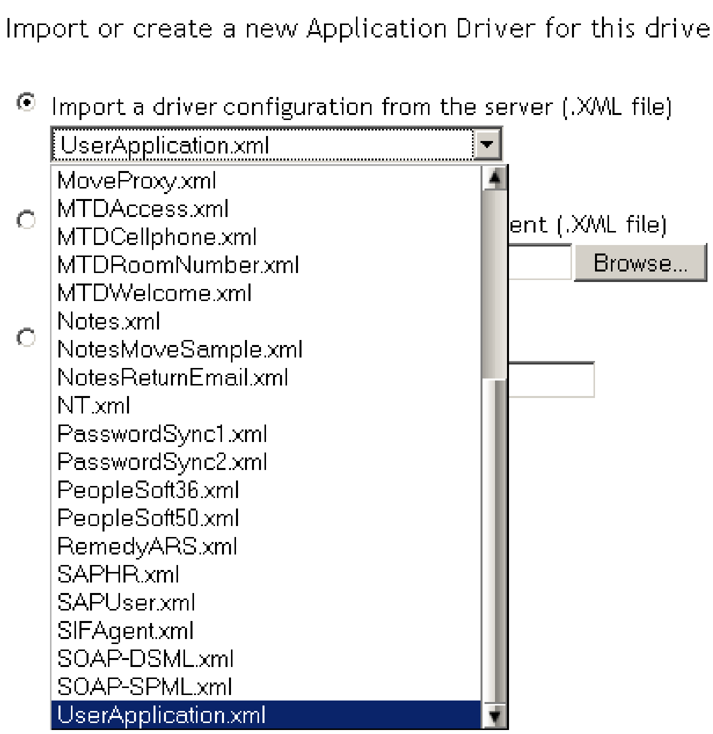
4 Se você selecionar *Em um conjunto de drivers existente*, um assistente será exibido e poderá ser usado para navegar no Cofre de Identidade e localizar o conjunto de drivers. Selecione o conjunto de drivers existente e selecione *Avançar.*

Se você selecionar *Em um novo conjunto de drivers*, uma tela será exibida e poderá ser usada para definir o novo conjunto de drivers. Especifique um nome, uma árvore de contexto e um servidor para o conjunto de drivers e selecione *Avançar*.

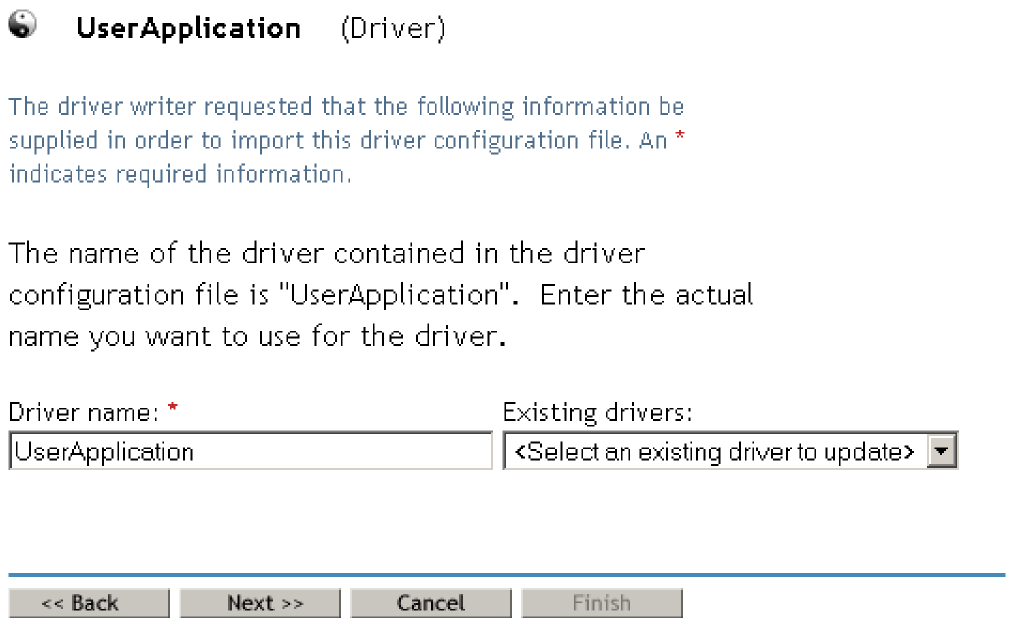
A próxima tela do *Assistente de Criação de Driver* é exibida:



5 Clique na opção *Importar configuração de driver do servidor* e selecione *UserApplication.xml* na lista de arquivos XML:



6 Clique em *Avançar*. O *Assistente de Criação de Driver* exibe uma página que você pode usar para nomear e configurar o driver:



O nome padrão do driver é UserApplication. Embora você possa usar o nome padrão, convém escolher um nome mais significativo ao seu projeto.

7 Se desejar, digite um novo nome para o driver no campo *Nome do driver*.

8 No campo *ID de Autenticação* , especifique o DN do administrador do aplicativo de usuário (consulte a Seção 1.1.2, "Administrador de Aplicativo de Usuário" na página 17 para obter uma descrição do administrador do aplicativo de usuário), usando o formato de pontos (por exemplo, admin.orgunit.novell).

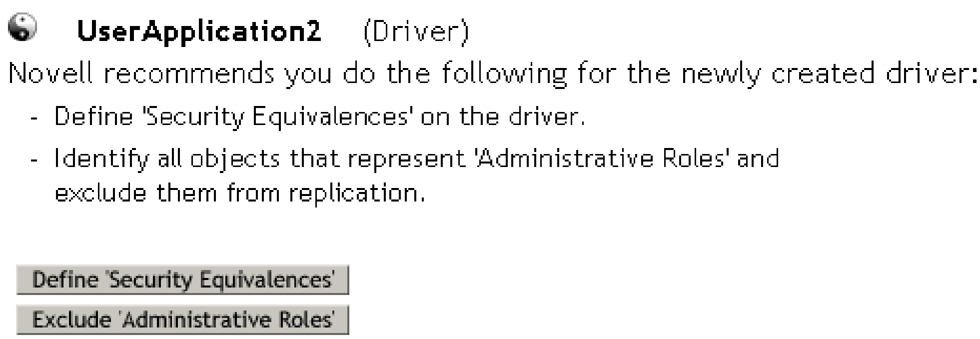
9 No campo *Senha do Aplicativo* e *Reinserir a senha*, especifique a senha do administrador do aplicativo de usuário identificado no campo *ID de Autenticação* .

10 No campo *Contexto do Aplicativo*, digite o nome do aplicativo especificado quando o aplicativo de usuário foi instalado. O nome padrão é `IDM`.

11 No campo *Host*, especifique o endereço IP ou o nome de host do servidor de aplicativos no qual o aplicativo de usuário é executado.

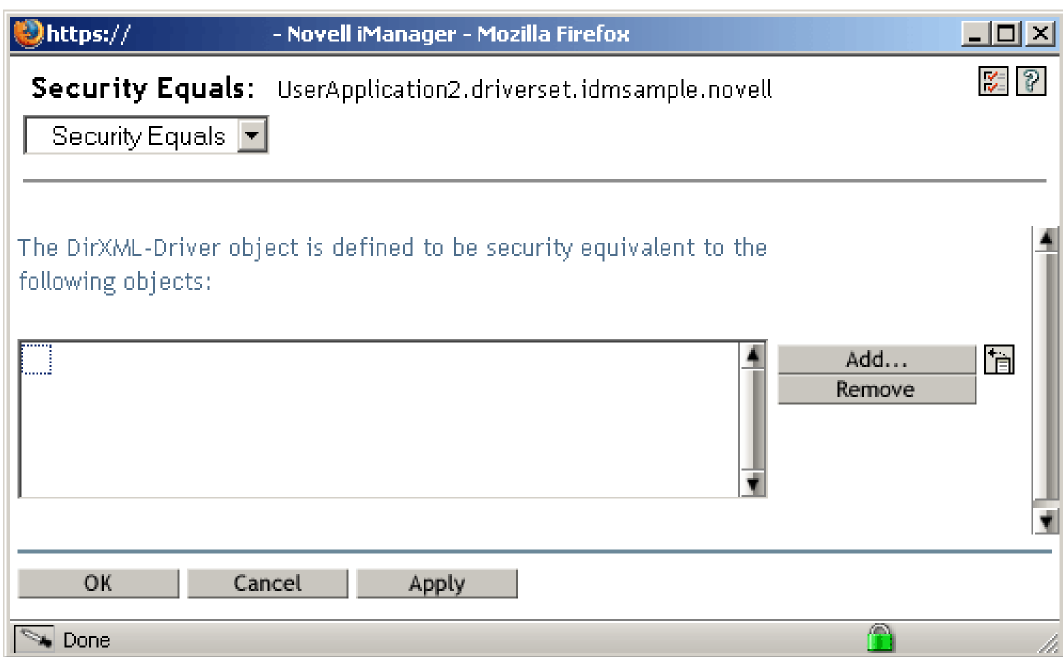
12 No campo *Porta*, especifique a porta através da qual o driver deverá se comunicar com o aplicativo de usuário sendo executado no servidor de aplicativos (por exemplo, 8088).

13 Clique em *Avançar*. É exibida uma mensagem para indicar que a configuração do driver está sendo importada. Em seguida, a página subseqüente do Assistente de *Criação de Driver* é exibida:

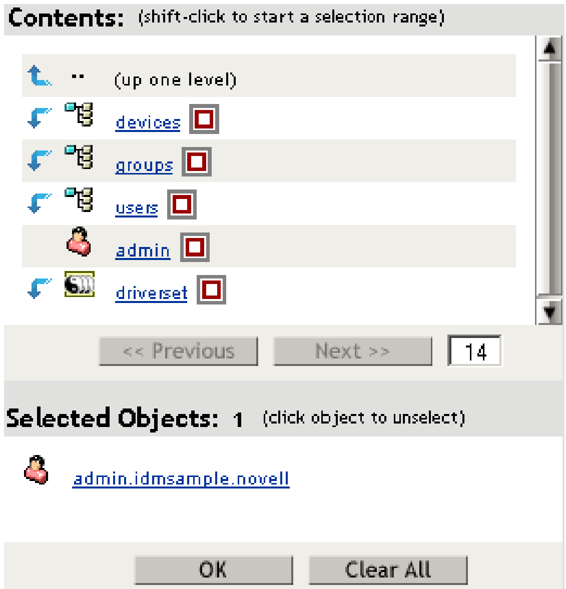


O objeto driver deve ter direitos suficientes em relação ao Cofre de Identidade para ler ou gravar qualquer objeto. Esses direitos podem ser definidos mediante a concessão de *Equivalências de Segurança* ao objeto driver. O driver deve ter acesso de Leitura/Gravação a usuários, agências postais, recursos e listas de distribuição, e de Criação, Leitura e Gravação ao container de agência postal. Geralmente, o driver deve apresentar o mesmo nível de segurança que o administrador.

14 Clique em *Definir Equivalência de Segurança*. Uma nova janela será exibida:



15 Clique em *Adicionar*. A janela exibida poderá ser usada para selecionar um objeto na árvore que tenha o nível de direitos apropriado que você deseja atribuir a esse driver (por exemplo, `admin`):



16 Selecione um objeto que tenha o nível de direitos de Cofre de Identidade desejado e clique em *OK*. Você voltará à janela anterior.

17 Clique em *OK*. Você voltará ao Assistente de *Criação de Driver*.

18 Clique em *Excluir Funções Administrativas*. A janela *Usuários Excluídos* será exibida. Use esse recurso para impedir que um administrador tenha seu acesso ao driver do aplicativo bloqueado, caso a senha do administrador seja mudada em outro Cofre de Identidade que seja replicado na árvore à qual esse driver pertence.

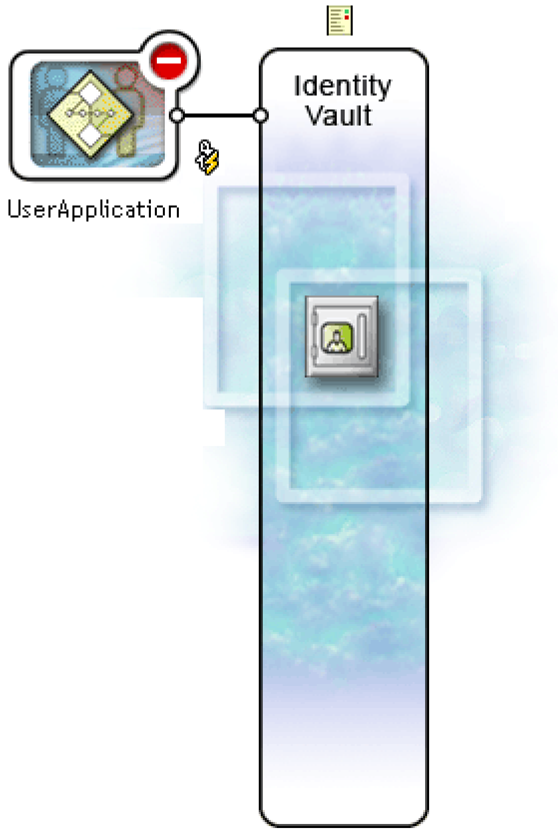
19 Clique em *Adicionar*. Será exibida uma janela em que você poderá pesquisar a árvore de diretório em busca de usuários cujos dados não deverão ser passados ao driver. Em geral, convém excluir objetos admin, uma vez que a replicação de seus dados através de uma conexão de driver não é uma prática recomendada na maioria dos cenários.

20 Selecione as funções administrativas que deseja excluir e clique em *OK*. Você voltará à janela anterior.

21 Clique em *OK*. Você voltará ao Assistente de *Criação de Driver*.

22 Clique em *Avançar.* Uma página de resumo do driver será exibida.

23 Clique em *Finalizar com Visão Geral*. É exibida uma representação gráfica do driver no Cofre de Identidade:



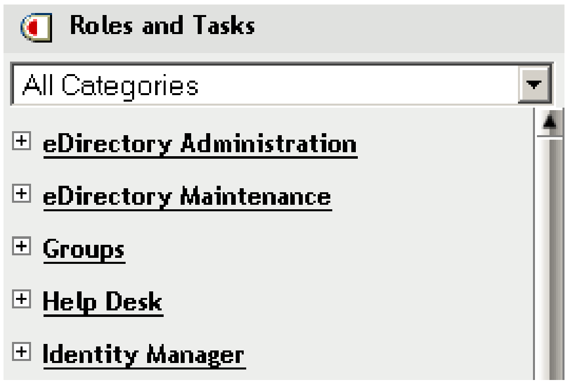
Observação: Você pode ver essa tela novamente a qualquer momento usando o link *Visão Geral do Identity Manager* em *Identity Manager* na árvore de navegação do iManager.

O novo driver é exibido como um ícone grande conectado à área do Cofre de Identidade.

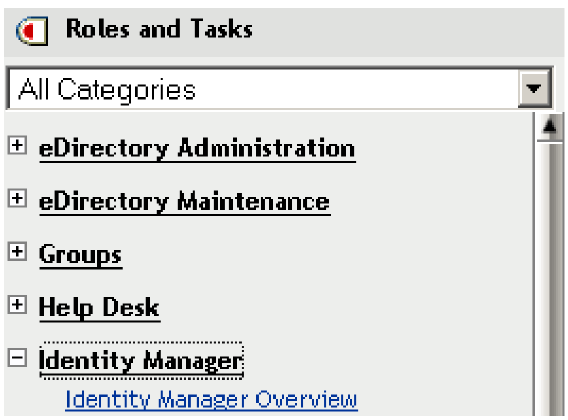
3.3 Iniciando o Driver de Aplicativo do Usuário

Para iniciar o driver de aplicativo do usuário:

1 Clique no link *Identity Manager* na árvore de navegação do iManager para ver os comandos disponíveis na categoria Identity Manager:



2 Clique no link *Visão Geral do Identity Manager* abaixo do link *Identity Manager* na árvore de navegação do iManager:



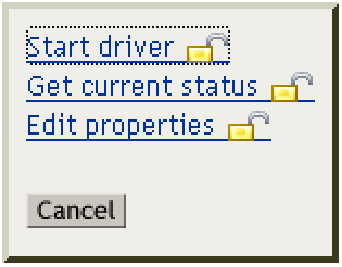
Será exibido um assistente que você poderá usar para pesquisar o sistema e localizar o conjunto de drivers que contém o driver a ser ativado.

3 Selecione o conjunto de drivers e clique em *Avançar.* A página *Visão Geral do Identity Manager* é exibida.

4 Clique no indicador de status redondo no canto superior direito do ícone de driver:



É exibido um menu que lista comandos para iniciar e interromper o driver, bem como editar suas propriedades:



5 Clique em *Iniciar driver*.

3.4 Configurando o início automático de workflows

Quando o módulo de aprovisionamento está instalado, os workflows são iniciados automaticamente assim que um usuário inicia uma solicitação de aprovisionamento ao solicitar um recurso. Além disso, o driver de aplicativo do usuário do Identity Manager tenta escutar se há eventos no Cofre de Identidade e, se estiver configurado para fazê-lo, responde aos eventos iniciando os workflows de aprovisionamento adequados. Por exemplo, você pode configurar o driver de aplicativo do usuário para iniciar automaticamente um workflow de aprovisionamento caso um novo usuário seja adicionado ao Cofre de Identidade. O driver de aplicativo do usuário pode ser configurado para iniciar automaticamente os workflows usando políticas e regras do Identity Manager.

3.4.1 Sobre políticas

Assim como faz com todos os drivers do Identity Manager, você pode usar filtros e políticas com o driver de aplicativo do usuário. Quando um evento ocorre no Cofre de Identidade, o Identity Manager cria um documento XML que o descreve. O documento XML é passado através do canal ao sistema conectado (nesse caso, o sistema conectado é o aplicativo de usuário). Filtros e políticas associados ao driver permitem definir como responder ao evento e, nesse processo, converter o documento XML para o formato esperado pelo sistema conectado. O Identity Manager fornece diversas categorias de política (por exemplo, Transformação de Eventos, Transformação de Comandos, Mapeamento de Esquema, Transformação de Saída) que podem ser aplicadas, de modo seqüencial, à conversão do documento XML. Nesta seção, fornecemos um exemplo de início de um workflow de acordo com eventos no Cofre de Identidade. Embora qualquer uma das políticas possa ser usada para acionar um workflow, esse exemplo demonstra o método mais fácil e útil.

Quando você cria um driver de aplicativo do usuário, uma Política de Transformação de Eventos é criada para o uso com esse driver. A Política de Transformação de Eventos é responsável pela criação do documento XML que será processado pelas demais políticas de canal do Assinante.

Observação: Não mude a Política de Transformação de Eventos criada quando o driver de aplicativo do usuário foi criado. O DN dessa política começa com `Manage.Modify.Subscriber`. A mudança dessa política poderá causar a falha do workflow.

Uma Política de Mapeamento de Esquema também é criada. Você pode usar essa política como ponto inicial para acionar um workflow de acordo com eventos no Cofre de Identidade.

3.4.2 Configurando o início de um workflow de acordo com um evento no Cofre de Identidade

O método mais simples de iniciar automaticamente um workflow é o uso do Editor de Política de Mapeamento de Esquema. O driver de aplicativo do usuário fornece uma política em branco a ser editada com esse fim.

O Editor de Política de Mapeamento de Esquema é usado para mapear atributos do Cofre de Identidade (incluindo o atributo *acionador* do eDirectory que, quando mudado, dá início ao workflow) aos dados de tempo de execução de um workflow de destino. Os dados de tempo de execução são determinados pelo gabarito de definição do workflow (consulte o Capítulo 22, “Configurando definições de solicitação de aprovisionamento” na página 321 para obter informações sobre gabaritos de definição de workflow). Os dados de tempo de execução são necessários para que um workflow seja concluído com êxito. Quando um workflow é criado, diversos *atributos globais* são criados no Cofre de Identidade e podem ser usados para personalizar o comportamento do driver de aplicativo do usuário. Um atributo global é um atributo que não pertence a qualquer classe de objeto Cofre de Identidade. Esses atributos são chamados <Nomeworkflow>_StartWorkflow, <Nomeworkflow>_recipient e <Nomeworkflow>_reason. Há também outros dois atributos que estão sempre presentes, chamados AllWorkflows:reason e AllWorkflows:recipient. O atributo _StartWorkflow é usado para iniciar um workflow. Os atributos _recipient e _reason são usados para aceitar dados de tempo de execução do Cofre de Identidade necessários ao workflow.

Para efetuar esse procedimento, você deverá saber o nome do atributo do Cofre de Identidade que deseja usar como acionador do workflow. Você deverá saber também o nome do workflow que deseja iniciar. Todos os workflows incluem um atributo especial nomeado `<Nomeworkflow>_StartApprovalFlow`. O início automático de um workflow como uma resposta a um evento no Cofre de Identidade pode ser configurado mapeando-se o atributo do eDirectory desejado ao atributo <Nomeworkflow>_StartApprovalFlow do workflow.

Para configurar o início de um workflow de acordo com um evento no Cofre de Identidade:

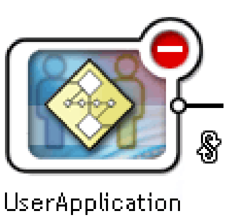
1 No iManager, clique no link *Visão Geral do Identity Manager* abaixo do link Identity Manager na árvore de navegação do iManager.



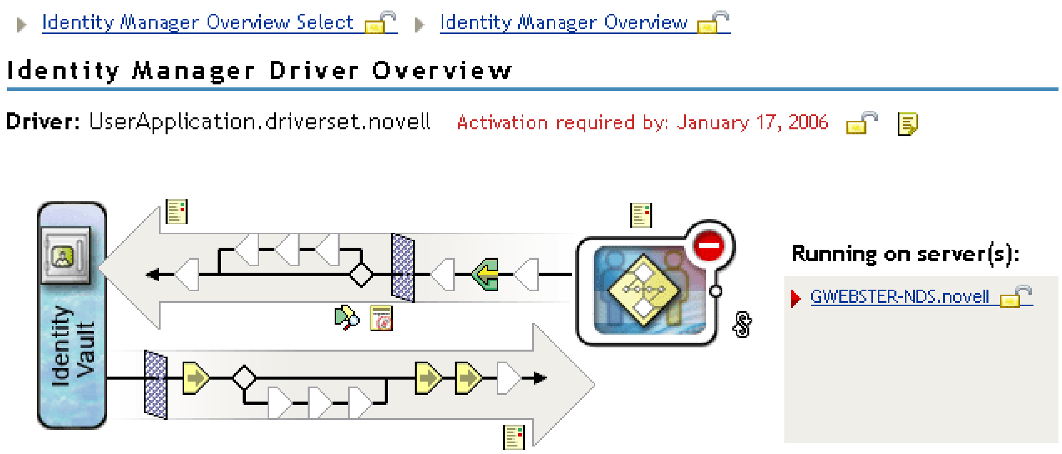
A página *Visão Geral do Identity Manager* é exibida. Essa página solicita que você selecione um conjunto de drivers.

2 Clique em *Pesquisar Árvore Toda*; em seguida, clique em *Pesquisar*. A página *Visão Geral do Identity Manager* é exibida com um gráfico que indica os drivers no conjunto de drivers selecionado naquele momento.

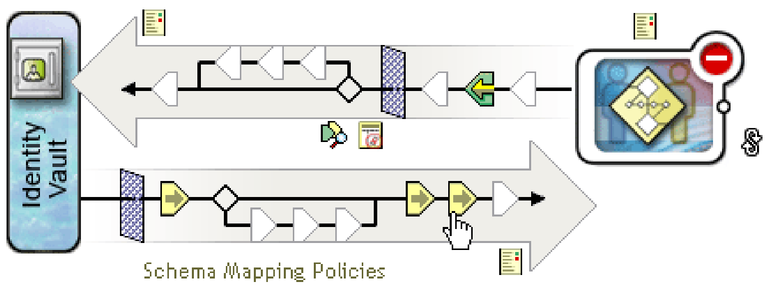
3 Clique no ícone grande do driver de aplicativo do usuário:



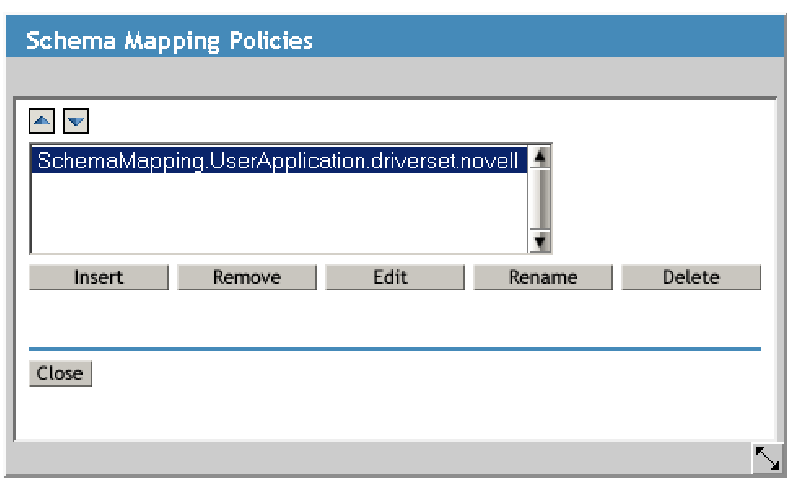
A página *Visão Geral do Driver do Identity Manager* é exibida:



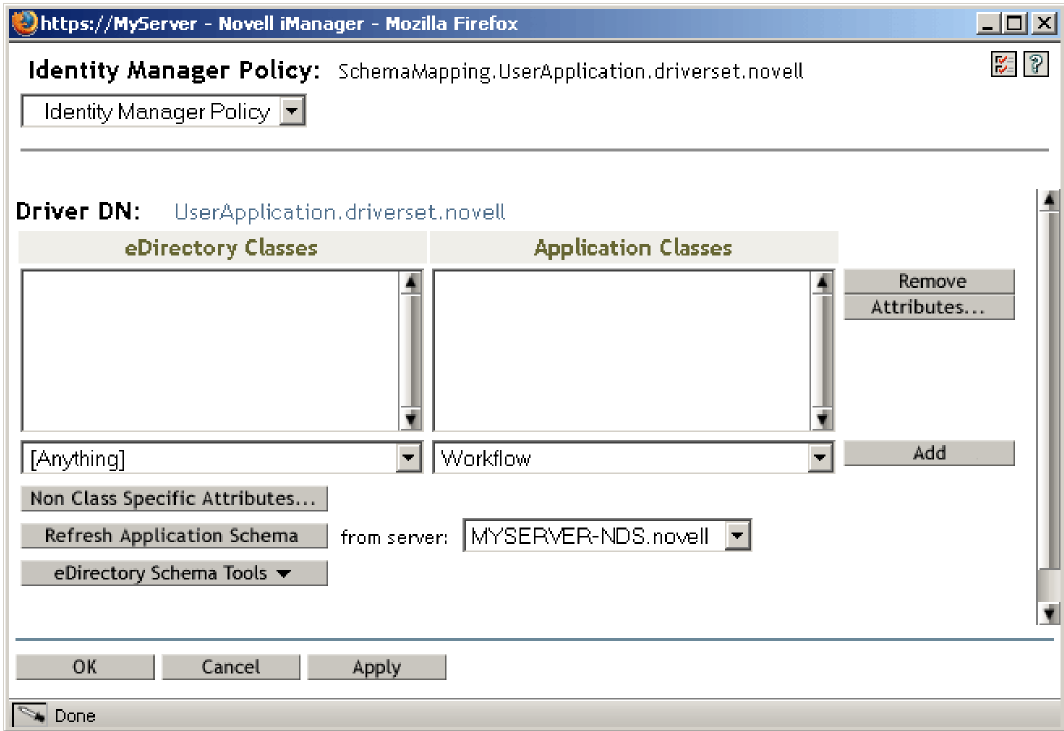
A seta horizontal superior representa o canal do Editor (que não é usado no driver de aplicativo do usuário) e a seta horizontal inferior representa o canal do Assinante. Quando você passa o ponteiro do mouse sobre um objeto no gráfico, sua descrição é exibida.



4 Clique no ícone *Políticas de Mapeamento de Esquema* do canal do Assinante. A caixa de diálogo *Políticas de Mapeamento de Esquema* é exibida, com o nome da política de mapeamento de esquema padrão realçado:



5 Clique em *Editar*. A caixa de diálogo *Política do Identity Manager* é exibida: Essa caixa de diálogo é usada para mapear classes do Cofre de Identidade a classes do aplicativo. Este procedimento não utiliza esse recurso. Em vez disso, ele mapeia atributos do eDirectory a atributos globais de aplicativo do usuário.

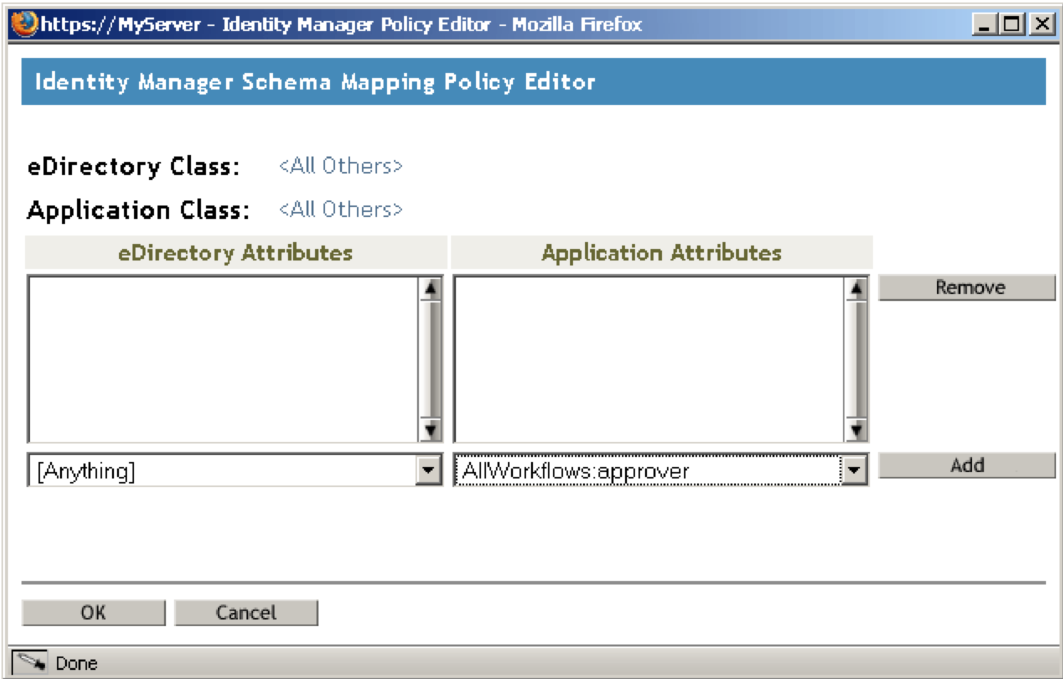


6 Clique em *Atualizar Esquema de Aplicativo*. É exibida uma mensagem para informar que o driver deve ser interrompido para ler o esquema e, em seguida, reiniciado. A atualização do esquema pode levar cerca de 60 segundos. Essa etapa lê o conjunto de informações de workflow mais recentes em preparação para a etapa seguinte, em que são especificadas as informações a serem movidas do Cofre de Identidade ao workflow a ser iniciado.

7 Clique em *OK* para atualizar o esquema. Uma mensagem será exibida quando o esquema tiver sido atualizado.

8 Clique em *OK* para fechar a mensagem sobre atualização do esquema. Você voltará à caixa de diálogo *Política do Identity Manager*.

9 Clique em *Atributos sem Classe Específica*. O *Editor de Política de Mapeamento de Esquema do Identity Manager* é exibido.



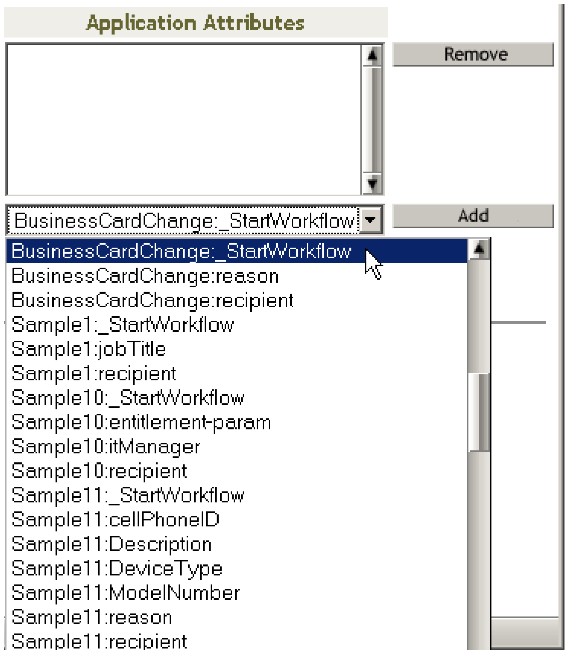
A lista suspensa *Atributos do eDirectory* contém todos os atributos do eDirectory.

A lista suspensa *Atributos do Aplicativo* contém os atributos em todos os workflows ativos. Os atributos na lista terão como prefixo `AllWorkflows` (o que significa que o atributo se aplica a todos os workflows), ou o nome de um workflow específico. Se você desejar que o mesmo atributo do eDirectory (por exemplo `gerente`) seja mapeado para o atributo `gerente` de todos os workflows, deverá mapear `gerente` para `Allworkflows:gerente`. Se você desejar que um atributo do eDirectory diferente (por exemplo `gerenteRH`) seja usado em um determinado workflow, deverá mapear o atributo do eDirectory para o atributo do workflow específico (por exemplo, `BusinessCardChange:gerente`).

Atributos que tenham sido mapeados são exibidos lado a lado nas colunas *Atributos do eDirectory* e *Atributos do Aplicativo*.

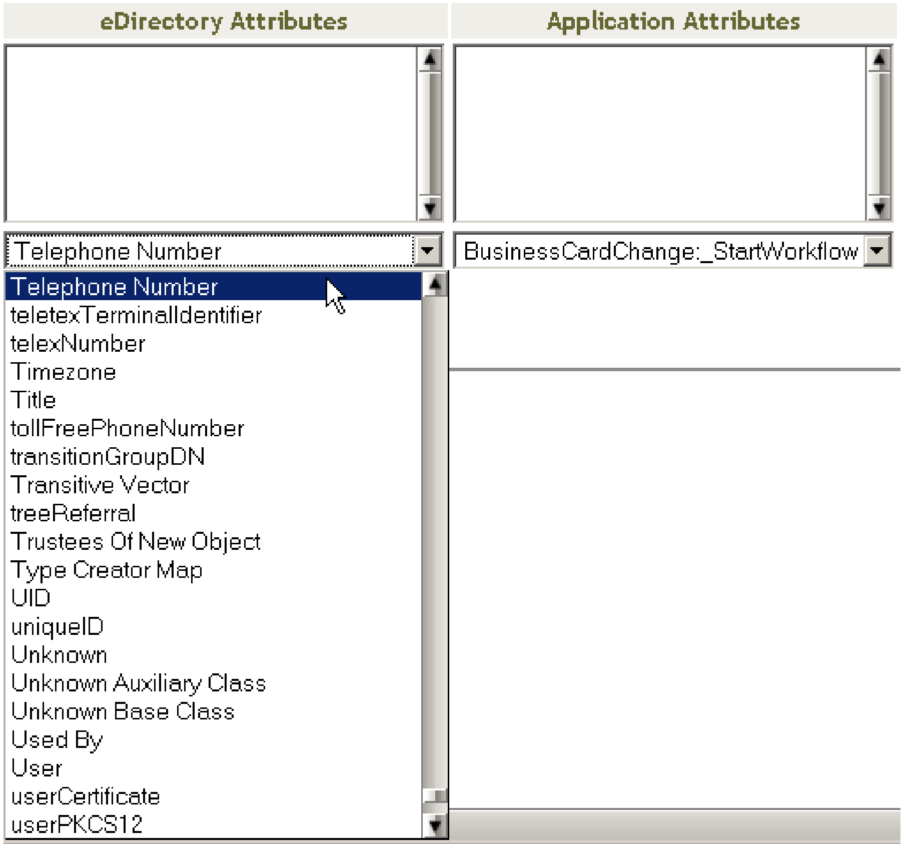
Nas etapas a seguir, você fará o mapeamento do atributo do eDirectory que deseja usar para iniciar o workflow ao atributo _StartWorkflow daquele workflow. Se atributos do eDirectory adicionais forem esperados pelo workflow, eles também deverão ser mapeados. Por exemplo, se um atributo `Endereço` do eDirectory for o acionador de um workflow, esse poderá exigir também atributos como `Cidade` e `Estado`. Alternativamente esses atributos podem ser mapeados em políticas.

10 Na lista *Atributos de Aplicativos*, selecione o atributo _StartWorkflow para o workflow a ser configurado. O exemplo a seguir mostra o atributo _StartWorkflow para um workflow BusinessCardChange (BusinessCardChange_StartWorkflow).

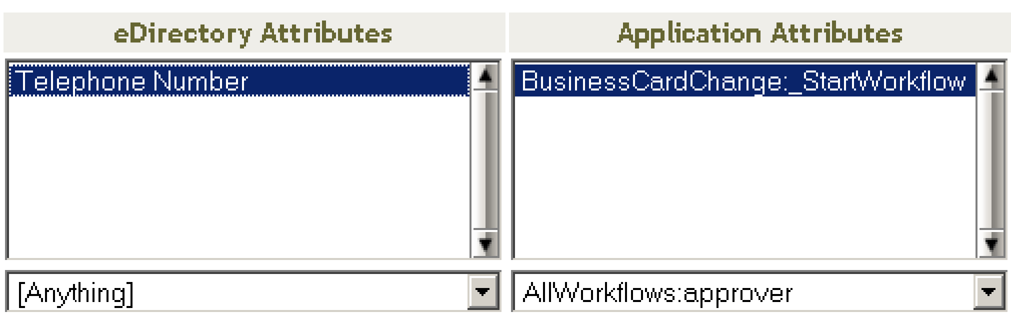


11 Na lista *Atributos do eDirectory*, selecione o atributo do eDirectory a ser usado para iniciar o workflow quando ocorrer mudança no atributo. No exemplo a seguir, o atributo Telephone está

selecionado. Isso significa que o workflow BusinessCardChange sempre terá início quando o número de telefone de um funcionário mudar.



12 Clique em *Adicionar*. O atributo do eDirectory está mapeado para o atributo Application.



13 Se o workflow precisar de atributos adicionais do eDirectory, repita da Etapa 10 à Etapa 12 até mapear todos os atributos desejados.

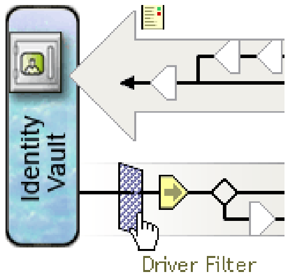
O workflow terá início automaticamente quando ocorrer uma mudança no atributo do eDirectory que está mapeado para um atributo application _StartApprovalFlow. Porém, o atributo do eDirectory só terá acesso à política de Mapeamento de Esquema se o atributo do eDirectory estiver incluído no filtro do driver do canal do Assinante. Nas próximas etapas, o atributo do eDirectory será adicionado ao filtro do driver do canal do Assinante

14 Clique em *OK* para fechar o *Editor de Política de Mapeamento de Esquema do Identity Manager*.

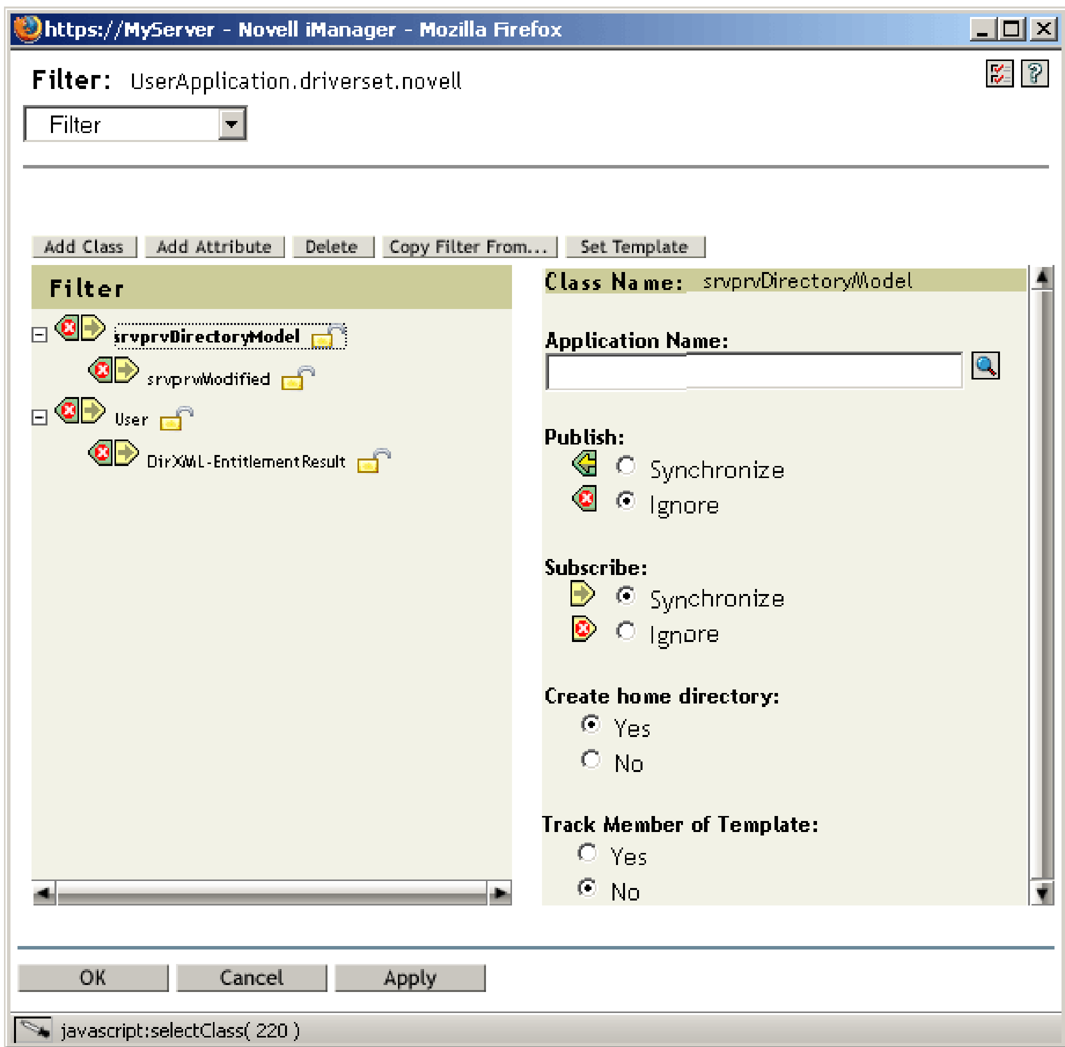
15 Clique em *OK* para fechar a caixa de diálogo *Identity Manager Policy*.

16 Clique em *Fechar* para fechar a caixa de diálogo Políticas de Mapeamento de Esquema.

17 Clique no ícone de *Filtro do Driver* do canal do Assinante.



A janela do filtro é exibida:



Os filtros do evento especificam as classes de objeto e os atributos para os quais o mecanismo do Identity Manager processa eventos. A lista apenas leitura *Filtro* à esquerda mostra os atributos da classe. A lista *Nome de Classe* à direita exibe opções associadas ao objeto-alvo.

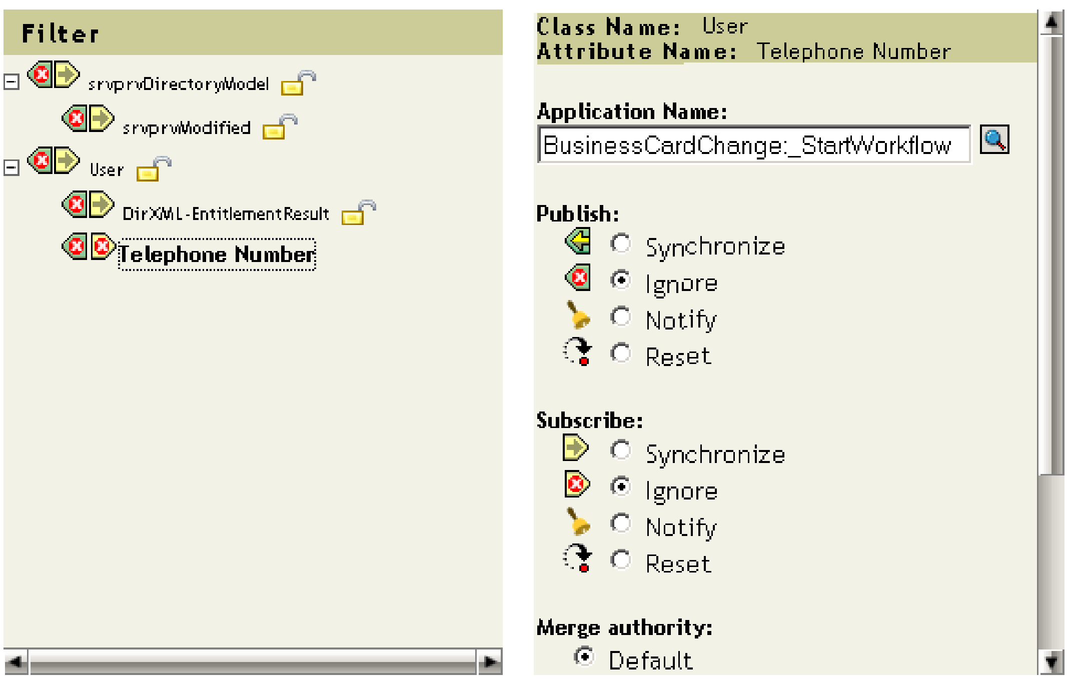
18 Clique no nome da classe à qual pertence o atributo a ser adicionado ao filtro (por exemplo, User).

19 Clique em *Adicionar Atributo*. Uma lista de atributos é exibida.

20 Selecione um Atributo e clique em *OK*. O atributo é adicionado à lista *Filtro*.



21 Clique no nome do atributo. As opções de sincronização do atributo são exibidas no painel à direita.



22 Em *Inscrever*, clique em *Sincronizar*.



23 Especifique todos os outros atributos do filtro. Selecione *Sincronizar* para um atributo se você quiser efetuar mudanças nos valores de atributo a serem informados e sincronizados. Selecione

Ignorar se você não quiser efetuar mudanças nos valores de atributo a serem informados e sincronizados.

24 Clique em *OK*. É exibida uma mensagem perguntando se você deseja que o driver seja reiniciado para ativar as mudanças.

25 Clique em *OK*. Você retornará à página *Visão Geral do Driver do Identity Manager*.

Configurando a Camada de Abstração do Diretório

4

Este capítulo descreve como usar o editor da camada de abstração do diretório para configurar as definições dos dados da camada de abstração do diretório usadas pelo aplicativo de usuário do Identity Manager. Os tópicos incluem:

4.1 Sobre as definições da camada de abstração do diretório

A *camada de abstração do diretório* é um conjunto de definições de dados que fornecem uma visão lógica de um cofre de identidade. A camada de definição do diretório define:

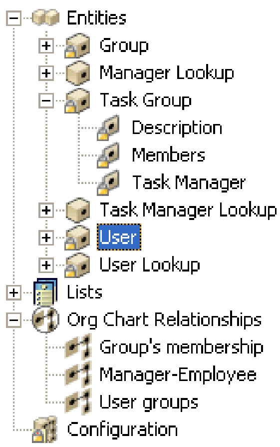
- Os atributos e os objetos do cofre de identidade que podem ser usados no aplicativo de usuário do Identity Manager.
- Como os dados do cofre de identidade são exibidos na interface de usuário.
- Os relacionamentos disponíveis para o portlet Organograma.

Você usará o *editor da camada de abstração do diretório* para mudar essas definições de dados, caso queira modificar a aparência ou a função do aplicativo de usuário. Você pode mudá-las da seguinte maneira:

- Adicionando outros objetos do cofre de identidade
- Mudando o conjunto de atributos disponíveis para um objeto do cofre de identidade
- Mudando o conteúdo de listas
- Mostrando diversos relacionamentos entre os objetos do cofre de identidade

O procedimento de instalação do aplicativo de usuário do Identity Manager instala e distribui o conjunto básico de definições da camada de abstração que são necessárias para que o aplicativo de usuário funcione corretamente. Essa instalação também cria extensões do esquema do eDirectory que são usadas pelo Driver de Aplicativo do Usuário e pelo aplicativo de usuário. Você pode obter mais informações sobre essas extensões de esquema no Apêndice A, "Extensões do esquema" na página 361. Esse mesmo conjunto básico de arquivos será criado no sistema de arquivos locais quando você criar uma nova instância do Driver de Aplicativo do Usuário por meio do Designer para Identity Manager.

Definições necessárias dos dados da camada de abstração Quando você começa a personalizar seu próprio aplicativo de usuário do Identity Manager, deseja efetuar mudanças nos objetos da camada de abstração do diretório. Entretanto, certos objetos do cofre de identidade (as chamadas entidades), atributos, relacionamentos e listas não podem ser removidos ou mudados, ou o aplicativo de usuário não funcionará corretamente. As definições que não podem ser removidas são identificadas por um ícone de cadeado. No exemplo, você vê que a entidade Grupo de Tarefas e todos os seus atributos são bloqueados.



Onde as definições da camada de abstração do diretório são armazenadas As definições da *camada de abstração do diretório* são arquivos XML:

- *Armazenados* localmente no sistema de arquivos do computador com o Designer no subdiretório Provisioning\AppConfig\DirectoryModel do projeto de aprovisionamento. Se houver mais de um Aplicativo de Usuário no projeto, os nomes de diretório serão numerados. Por exemplo, AppConfig1, AppConfig2 e assim por diante.
- *Distribuídos* no container AppConfig.DirectoryModel do Driver de Aplicativo do Usuário. Os arquivos XML são armazenados no atributo XMLData do objeto de definição da camada de abstração do diretório correspondente. Cada entidade, relacionamento e lista é uma instância de objeto exclusiva contida no container AppConfig.DirectoryModel do Driver de Aplicativo do Usuário.
- *Armazenados no cache* do servidor onde o aplicativo de usuário é distribuído.

4.2 Operações iniciais

Você usará os recursos do modo de aprovisionamento do Designer para Identity Manager e o editor da camada de abstração do diretório para definir o conteúdo da camada de abstração do diretório. Siga estas etapas para começar:

Etapa	Tarefa	Descrição
1	Criar um projeto do Identity Manager	Isso inclui: ◆ Configurar o Cofre de Identidade ◆ Especificar as propriedades do Conjunto de Drivers Consulte a documentação do Identity Manager.
2	Adicionar um driver de Aplicativo do Usuário ao Modeler	O Driver de Aplicativo do Usuário do Identity Manager pode ser encontrado na pasta Provisioning da Paleta do Modeler. 
3	Concluir a configuração do Driver de Aplicativo do Usuário	Verifique o procedimento da Seção 4.2.1, “Concluindo a configuração do Driver de Aplicativo do Usuário” na página 77.
4	Acessar o modo de aprovisionamento	Consulte a Seção 4.2.2, “Acessando o modo de aprovisionamento” na página 81.)
5	Iniciar o editor da camada de abstração do diretório	Consulte “Para abrir o editor da camada de abstração do diretório:” na página 82.)

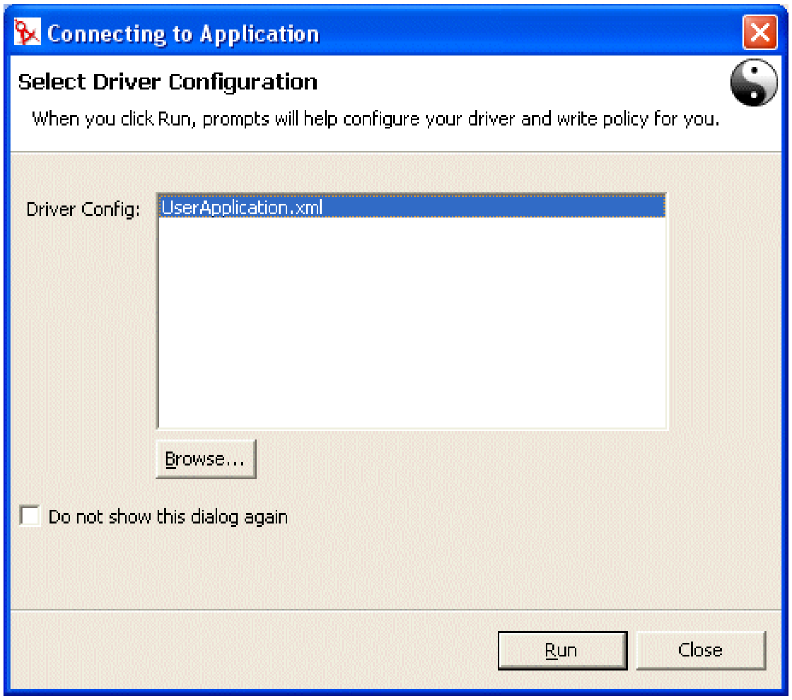
4.2.1 Concluindo a configuração do Driver de Aplicativo do Usuário

Siga estas etapas depois de criar um projeto do Identity Manager.

Para concluir a configuração do Driver de Aplicativo do Usuário:

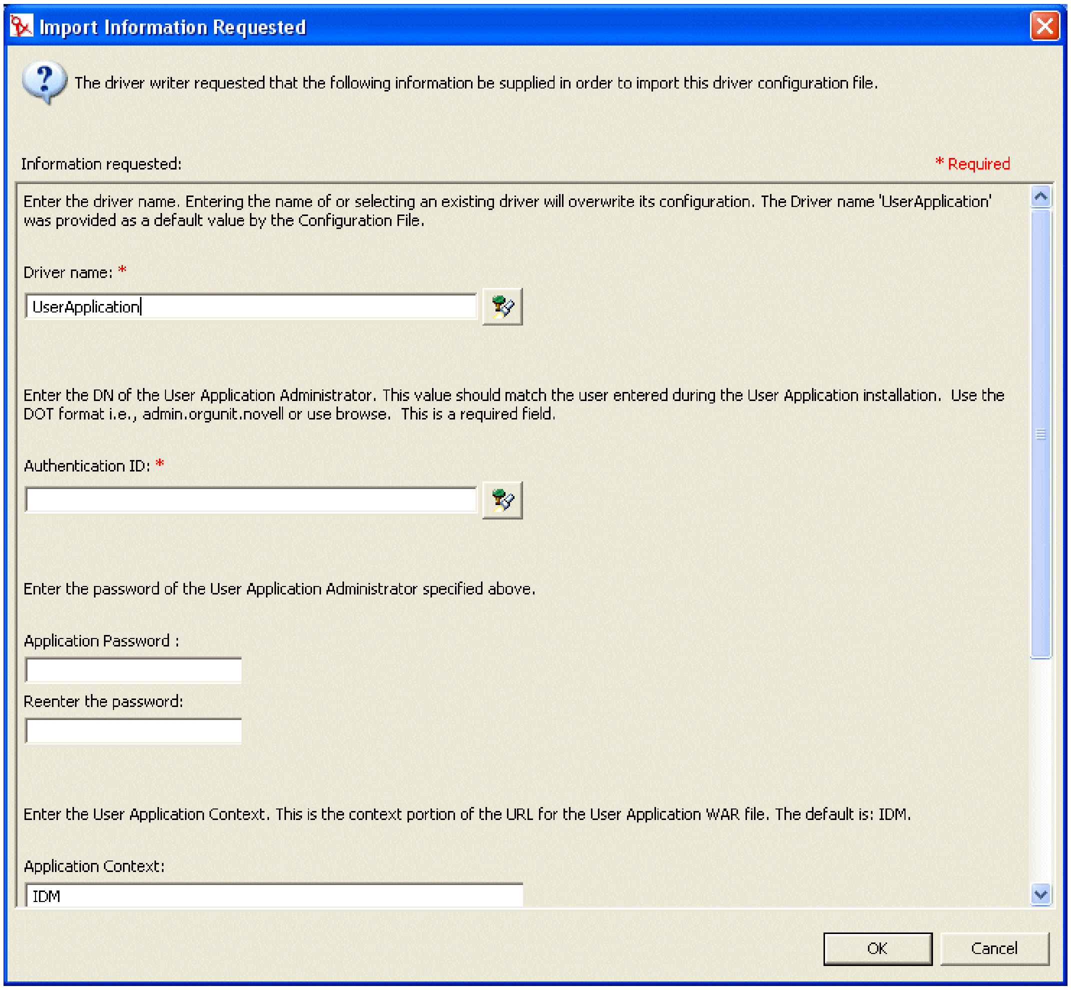
1 Coloque um ícone do driver de *Aplicativo do Usuário* na tela.

Você será solicitado a informar a configuração do driver.



2 Selecione *UserApplication.xml* (o padrão) e clique em *Executar*.

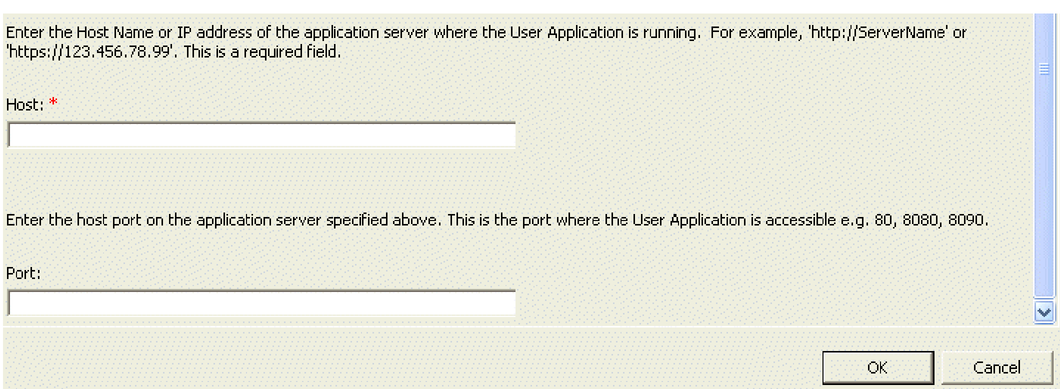
3 Clique em Sim ou Não para especificar como o assistente deve tratar a validação das entradas.



.

.

.



4 Preencha o painel da seguinte maneira:

Propriedade	O que especificar
Nome do Driver	◆ O nome de um driver existente (o driver do conjunto que foi especificado durante a instalação do aplicativo de usuário). ◆ O nome de um novo driver.
ID de Autenticação	O DN do Administrador de Aplicativo de Usuário.
Senha do aplicativo/Digite novamente a senha	A senha do Administrador de Aplicativo de Usuário (acima).
Contexto do aplicativo	O nome do contexto do aplicativo de usuário (especificado na instalação. Por exemplo, IDM).
Host	O nome de host ou o endereço IP do servidor onde o aplicativo de usuário do Identity Manager foi distribuído. Essa informação é usada: ◆ Para acionar workflows no servidor de aplicativos para conexão e acesso a workflows (terminar, recolher e assim por diante). ◆ Para atualizar as definições de dados armazenadas em cache.
Porta	A porta do host acima.

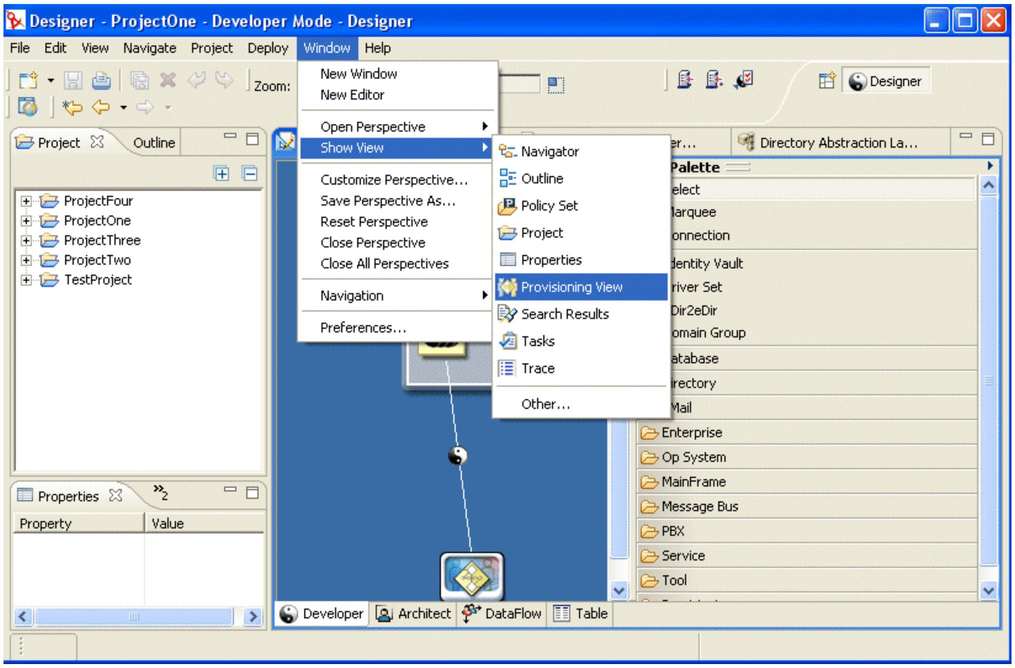
5 Clique em *OK*.

4.2.2 Acessando o modo de aprovisionamento

Para acessar o modo de aprovisionamento

1 Escolha uma destas opções:

- Selecione *Janela>Mostrar Tela>Modo de Aprovisionamento*.



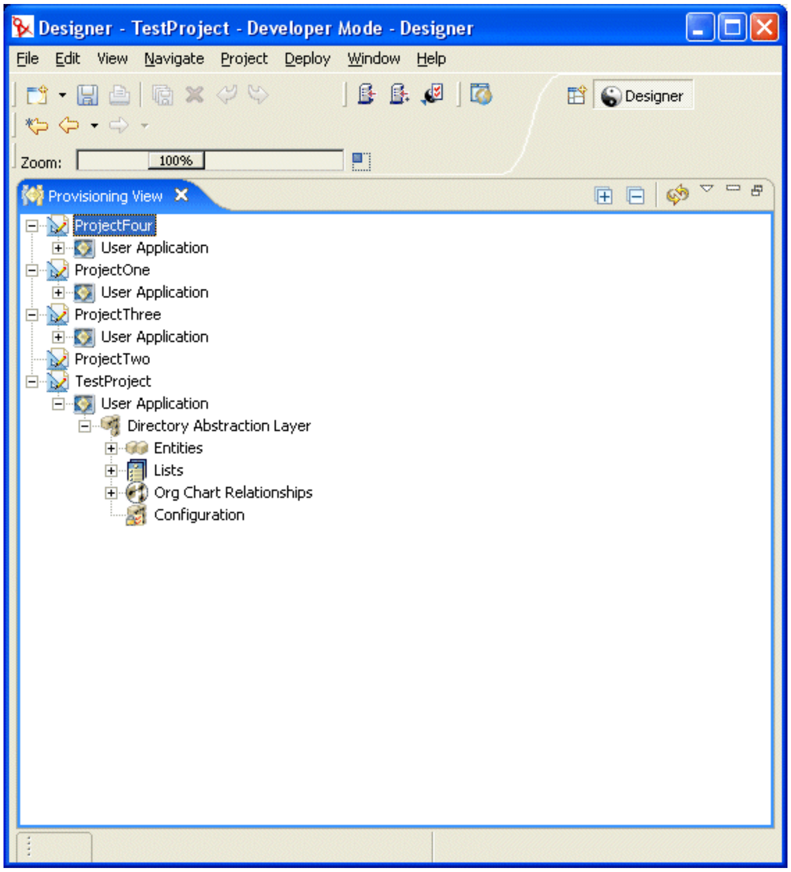
- Abra a pasta *Provisioning* e selecione *Modo de Aprovisionamento*.
- Clique em *OK*.

ou

- Selecione o ícone do Aplicativo de Usuário, clique o botão direito do mouse e selecione *Aplicativo>Mostrar Modo de Aprovisionamento*.

No modo de aprovisionamento, você verá o projeto recém-criado e outros projetos de aprovisionamento na mesma área de trabalho.

Dica: Se você não encontrar os aplicativos no modo de exibição, *pode* ser que o projeto esteja danificado. Se o projeto estiver danificado, será preciso recriá-lo.



Sobre o modo de aprovisionamento

O modo de aprovisionamento oferece acesso persistente aos recursos de aprovisionamento. Clique duas vezes em um item no modo de aprovisionamento para abrir o editor desse item. No modo de aprovisionamento, você executa as seguintes ações com as definições da camada de abstração do diretório:

- *Importar* uma ou mais definições de objeto do cofre de identidade.
- *Validar* a estrutura das definições de dados.
- *Distribuir* suas definições no cofre de identidade especificado no projeto.
- *Criar e apagar* definições da camada de abstração do diretório.

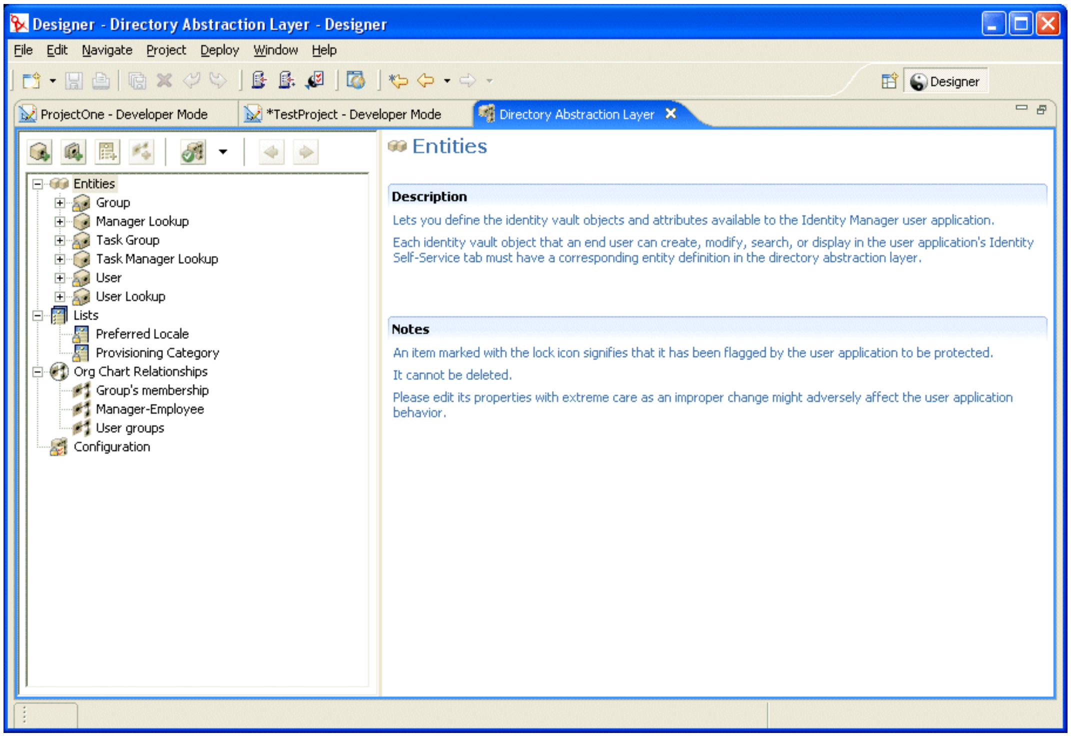
Para obter mais informações, consulte a Seção 4.8, “Importando, validando e distribuindo definições da camada de abstração do diretório” na página 111.

4.2.3 Iniciando o editor da camada de abstração do diretório

Para abrir o editor da camada de abstração do diretório:

1. Com o *modo de aprovisionamento* aberto, navegue até o nó da Camada de Abstração do Diretório.
2. Clique duas vezes no nó da Camada de Abstração do Diretório.

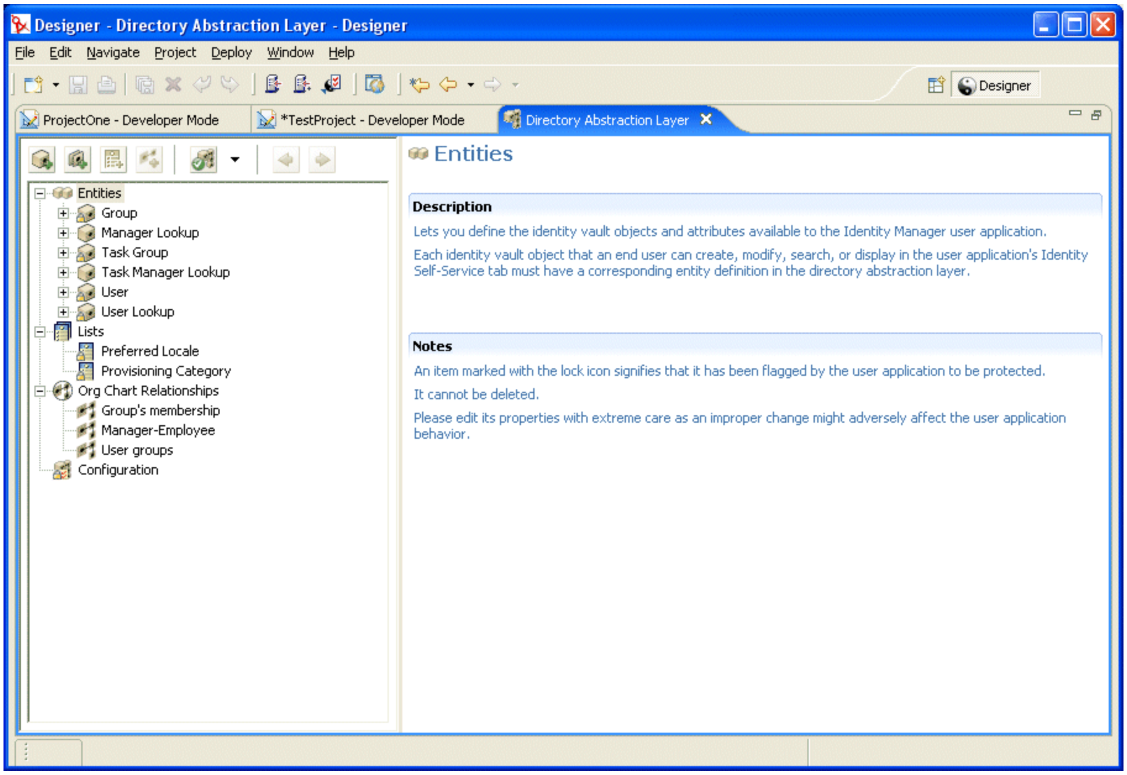
Você verá uma árvore com Entidades, Listas, Relacionamentos de Organogramas e Configuração.



Sobre o editor da camada de abstração do diretório

O editor da camada de abstração do diretório oferece um meio gráfico de definir o conjunto de arquivos XML que compõem a camada de abstração do diretório. O editor da camada de abstração do diretório é uma ferramenta com base em Eclipse que você pode acessar no *modo de aprovisionamento* de um projeto do Identity Manager.

Quando você abrir o editor da camada de abstração do diretório pela primeira vez, verá um conjunto básico de objetos dessa camada que são criados automaticamente toda vez que você gera um novo projeto de aprovisionamento:



Os nós do editor da camada de abstração do diretório incluem:

Elemento	Descrição
Entidades	As entidades representam os objetos do cofre de identidade configurados para esse projeto e disponíveis para o aplicativo de usuário. Há dois tipos de entidades: ◆ **Entidades que são mapeadas do esquema**. Elas representam os objetos que existem no cofre de identidade que ficam expostos diretamente ao usuário através do aplicativo de usuário. Normalmente, os usuários podem criar, pesquisar e modificar os atributos desses tipos de objetos. ◆ **Entidades que representam relacionamentos LDAP**. Também são conhecidas como DNLookups. Elas representam pesquisas indexadas e são usadas para dar suporte a determinados tipos de atributos que você deseja expor. As entidades DNLookup fornecem informações sobre relacionamentos entre objetos LDAP. Essas entidades são usadas pelos seguintes itens: ◆ Portlet Organograma para determinar relacionamentos. ◆ Os portlets Lista de Pesquisa, Criar e Detalhes para fornecer listas de seleção popup e contextos DN. Para obter mais informações, consulte a Seção 4.3.3, “Definindo entidades” na página 88.
Listas	Permite definir o conteúdo de listas globais. As listas globais são: ◆ Associadas a um atributo. O atributo é exibido no aplicativo de usuário como uma lista suspensa. ◆ Elas são usadas para exibir categorias utilizadas pelo Provisioning Request Configuration Plug-in do iManager. Para obter mais informações, consulte a Seção 4.4, “Trabalhando com listas” na página 103.
Relacionamentos de Organograma	Usado pela ação Organograma da guia Auto-atendimento de Identidade do aplicativo de usuário. Possibilita o mapeamento de relacionamentos hierárquicos entre entidades baseadas em esquema. Para obter mais informações, consulte a Seção 4.5, “Trabalhando com relacionamentos de Organograma” na página 106.
Configuração	Parâmetros de configuração geral Para obter mais informações, consulte a Seção 4.6, “Trabalhando com definições de configuração” na página 109.

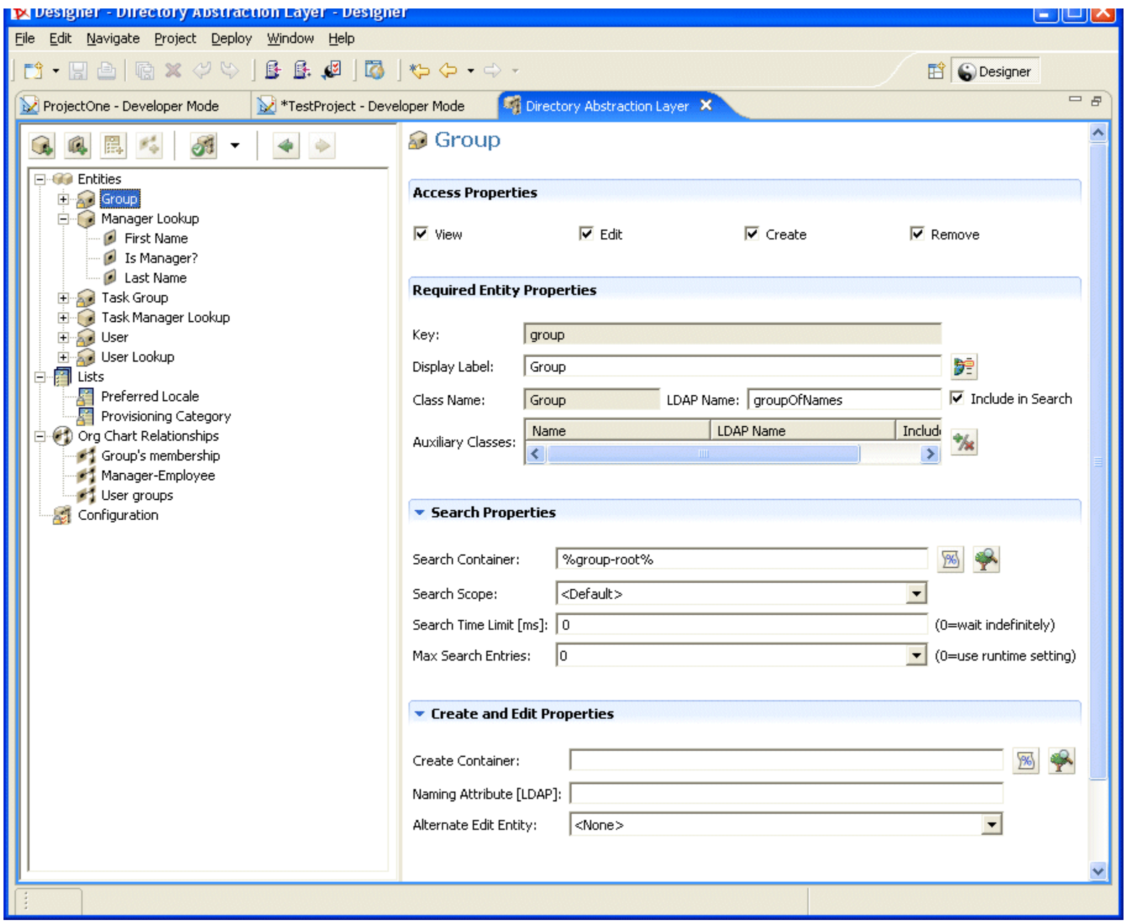
Onde os arquivos XML são armazenados localmente O editor da camada de abstração do diretório gera um arquivo XML para cada entidade, lista ou relacionamento. Os arquivos são armazenados na pasta Provisioning\AppConfig\DirectoryModel do projeto. O nome do arquivo baseia-se na chave do objeto. Estão incluídos:

Diretório	Descrição
ChoiceDefs	Contém os arquivos que definem as listas globais. Os arquivos têm a extensão .choice.
EntityDefs	Contém os arquivos que definem as entidades e os atributos. Os arquivos têm a extensão .entity.
RelationshipDefs	Contém os arquivos que definem os relacionamentos disponíveis para o portlet Organograma. Esses arquivos têm a extensão .relation.

Você usará os recursos do editor da camada de abstração do diretório para adicionar novas definições que modelam seu próprio esquema do cofre de identidade. Você usará os recursos do *modo de aprovisionamento* para distribuir as novas definições para o cofre de identidade.

Usando o editor da camada de abstração do diretório

O editor da camada de abstração do diretório divide-se em dois painéis. O painel esquerdo permite visualizar o conteúdo da camada de abstração do diretório. Quando você seleciona um item no painel esquerdo, o painel direito exibe os atributos e as configurações do item selecionado.



4.3 Trabalhando com entidades e atributos

Todo objeto do cofre de identidade que você quiser que os usuários pesquisem, exibam ou editem no aplicativo de usuário do Identity Manager deve ser definido como uma *entidade* na camada de abstração do diretório. Por exemplo, para usar o objeto do cofre de identidade inetOrgPerson no aplicativo de usuário, você deve criar uma definição de entidade para ele.

4.3.1 Etapas para adicionar entidades

Siga estas etapas para adicionar entidades à camada de abstração do diretório:

Etapa	Tarefa	Para obter mais informações
1	Escolher os objetos do cofre de identidade que você deseja usar no aplicativo de usuário.	Seção 4.3.2, “Analisando suas necessidades de dados” na página 87
2	Usar o editor da camada de abstração do diretório para definir os objetos do cofre de identidade na camada de abstração do diretório	Seção 4.3.3, “Definindo entidades” na página 88
3	Usar o modo de aprovisionamento para validar as definições de dados	Seção 4.8, “Importando, validando e distribuindo definições da camada de abstração do diretório” na página 111
4	Distribuir as definições no cofre de identidade	Seção 4.8.3, “Sobre a distribuição” na página 114
5	Atualizar o cache do servidor de aplicativos para incluir novas definições da camada de abstração	Capítulo 13, “Configuração de cache” na página 217
6	Testar o aplicativo de usuário do Identity Manager para verificar se suas mudanças são exibidas corretamente	

4.3.2 Analisando suas necessidades de dados

Para modelar os dados do cofre de identidade na camada de abstração do diretório, você precisa saber:

- As *partes do diretório* que você deseja colocar disponíveis para o aplicativo de usuário do Identity Manager.

Por exemplo, a lista de objetos que o usuário pode pesquisar e exibir. Compare essa lista com o conjunto básico de definições da camada de abstração para determinar o que precisa ser adicionado.

- A *estrutura do esquema* incluindo extensões personalizadas e classes auxiliares
- A *estrutura dos dados*, inclusive:
    - O que é necessário e o que é opcional
    - Regras de validação
    - Relacionamentos entre objetos (referências DN)
    - Como os atributos são definidos (por exemplo, um atributo que representa um número telefônico pode ter diversos valores para casa, escritório e celular)

- Quem verá os dados

  O site é público ou privado?

Use essas informações para mapear os objetos do cofre de identidade para entidades da camada de abstração.

Observação: As ACLs do eDirectory aplicam-se a todos os objetos da camada de abstração. Os direitos efetivos sobre objetos e atributos baseiam-se no usuário autenticado no momento do login no aplicativo.

4.3.3 Definindo entidades

Dependendo do que será exposto no aplicativo de usuário, você definirá dois tipos de entidades:

- *Entidades que são mapeadas do esquema*. Elas representam os objetos que existem no cofre de identidade que ficam expostos diretamente no usuário através do aplicativo de usuário. Ao definir esse tipo de identidade, você exporá todos os atributos com os quais deseja que os usuários trabalhem. Estes são alguns exemplos de tipo de entidade: Usuário, Grupo e Grupo de Tarefas. Você também pode criar mais de uma definição de entidade para o mesmo objeto se quiser expor diversos conjuntos de atributos para diferentes tipos de usuários. Para obter mais informações, consulte "Criar diversas definições de entidade para um objeto" na página 88.
- *Entidades que representam relacionamentos LDAP*. Esse tipo de entidade é conhecida como DNLookup e é usada pelo aplicativo de usuário para:
  - Preencher uma lista com os resultados de uma pesquisa DN entre as entidades relacionadas
  - Manter a integridade referencial entre atributos de referência DN durante atualizações e exclusões

  As entidades que dão suporte a DNLookups são usadas pelo portlet Organograma para determinar relacionamentos e também são usadas pelos portlets Pesquisar, Criar e Detalhes para fornecer listas de seleção popup e contextos DN. Estes são exemplos do tipo de entidade: Pesquisa de Gerente, Pesquisa de Gerenciador de Tarefas e Pesquisa de Usuário. Para obter mais informações, consulte "Usando tipos de controle DNLookup" na página 100.

Criar diversas definições de entidade para um objeto

Você pode criar mais de uma definição de entidade que represente o mesmo objeto do cofre de identidade mas que ofereça uma visualização diferente dos dados. Nas definições de entidade, é possível:

- *Definir diferentes atributos* para cada definição de entidade

OU

- *Definir os mesmos atributos*, mas especificar diversas propriedades de acesso que controlam como os atributos são pesquisados, visualizados, editados ou ocultos

---

Observação: Opcionalmente, as definições de entidade podem incluir um filtro para ocultar certas entidades do conjunto de resultados.

Em seguida, você pode usar essas diversas definições de identidade em várias partes da interface de usuário. Por exemplo, suponha que você queira criar um diretório de funcionários; um para um site público e outro para um site interno. No site público, você pretende informar o nome e sobrenome e um número de telefone. No site interno, você deseja relacionar informações adicionais como cargo, gerentes e assim por diante. Proceda da seguinte maneira para fazer isso:

1 Crie duas definições de entidade (com chaves diferentes).

   As duas definições expõem o mesmo objeto do cofre de identidade, mas uma chave da definição de identidade são informações públicas sobre a equipe, e a outra consiste em informações internas.

2 Em cada definição de entidade, estipule um conjunto distinto de atributos: um para informações públicas sobre a equipe, e outro para informações internas.

3 Use a guia Administração do Portal do aplicativo de usuário do Identity Manager para criar uma instância de portlet para a página pública, e outra para a página interna.

   Para obter mais informações sobre como criar instâncias de portlet, consulte Capítulo 9, “Administração de Portlet” na página 179.

Procedimentos para criar definições de entidade

Depois de determinar as entidades e os atributos a serem expostos, você pode começar a adicioná-los à camada de abstração do diretório usando o editor. Você seguirá um conjunto de etapas como este:

Etapa	O que fazer	Verifique este procedimento
1.	Escolha o conjunto de arquivos com os quais deseja começar.	
	◆ Você deseja adicioná-los ao conjunto básico de definições	Seção 4.3.1, “Etapas para adicionar entidades” na página 87
	◆ Você deseja começar com as definições já distribuídas	Seção 4.8.1, “Sobre como importar” na página 111
1a.	Algumas entidades que você pretende usar não integram o esquema de base do eDirectory. As extensões do esquema do eDirectory não serão exibidas automaticamente na lista do editor de objetos e atributos selecionáveis. Isso significa que você precisa atualizar o arquivo de esquema local do Designer para incluir esses objetos e atributos personalizados.	“Para atualizar a lista de elementos de esquema disponíveis:” na página 89
2.	Adicione uma ou mais entidades à camada de abstração do diretório	“Adicionando entidades” na página 90
3.	Adicione atributos às entidades	“Adicionando atributos” na página 93

Atualizando a lista de elementos de esquema disponíveis

Para atualizar a lista de elementos de esquema disponíveis:

1 Com o projeto do Identity Manager aberto, selecione o Cofre de Identidade, clique o botão direito do mouse e selecione *Operações Ativas>Importar Esquema*.

2 Escolha *Importar do eDirectory* e forneça as especificações para o host do eDirectory.
3 Clique em *Avançar*.
4 Selecione as classes e os atributos a serem importados e clique em *Concluir*.

Adicionando entidades

Você pode adicionar entidades com o assistente para adicionar entidade (descrito em seguida) ou clicando no botão *Adicionar Entidade* na barra de ferramentas do editor.

Observação: Quando você usa o botão Adicionar Entidade, precisa selecionar a classe de objeto da entidade a ser criada. O editor adiciona automaticamente os atributos necessários à entidade. Você usa a caixa de diálogo Adicionar Atributo para concluir a definição da entidade.

Para adicionar uma entidade usando o assistente para adicionar entidade:

1 Inicie o assistente para adicionar entidade de uma das seguintes maneiras:

No *modo de aprovisionamento*:

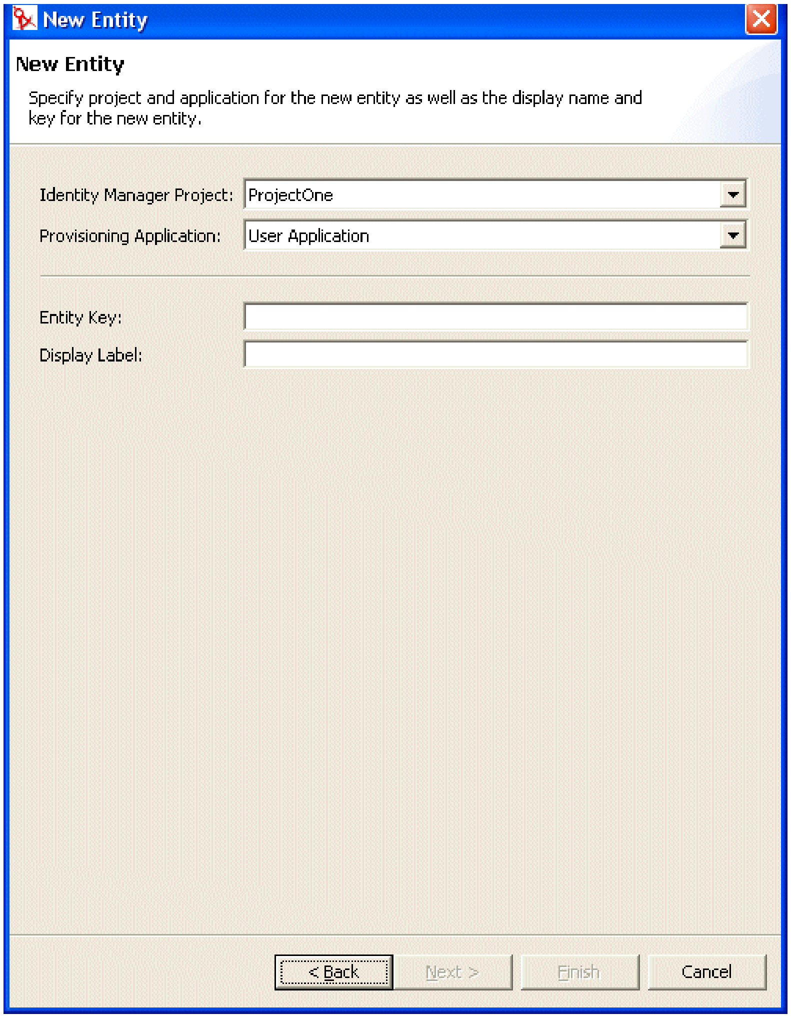
- Selecione o nó *Entidades*, clique o botão direito do mouse e escolha *Novo*.
- Selecione *Arquivo>Novo>Aprovisionamento*. Escolha *Entidade da Camada de Abstração do Diretório*. Clique em *Avançar*.

No editor da camada de abstração do diretório:

- Selecione o nó *Entidades*, clique o botão direito do mouse e escolha *Assistente de Novos Atributos e Entidades*.

  A caixa de diálogo Nova Entidade é exibida.

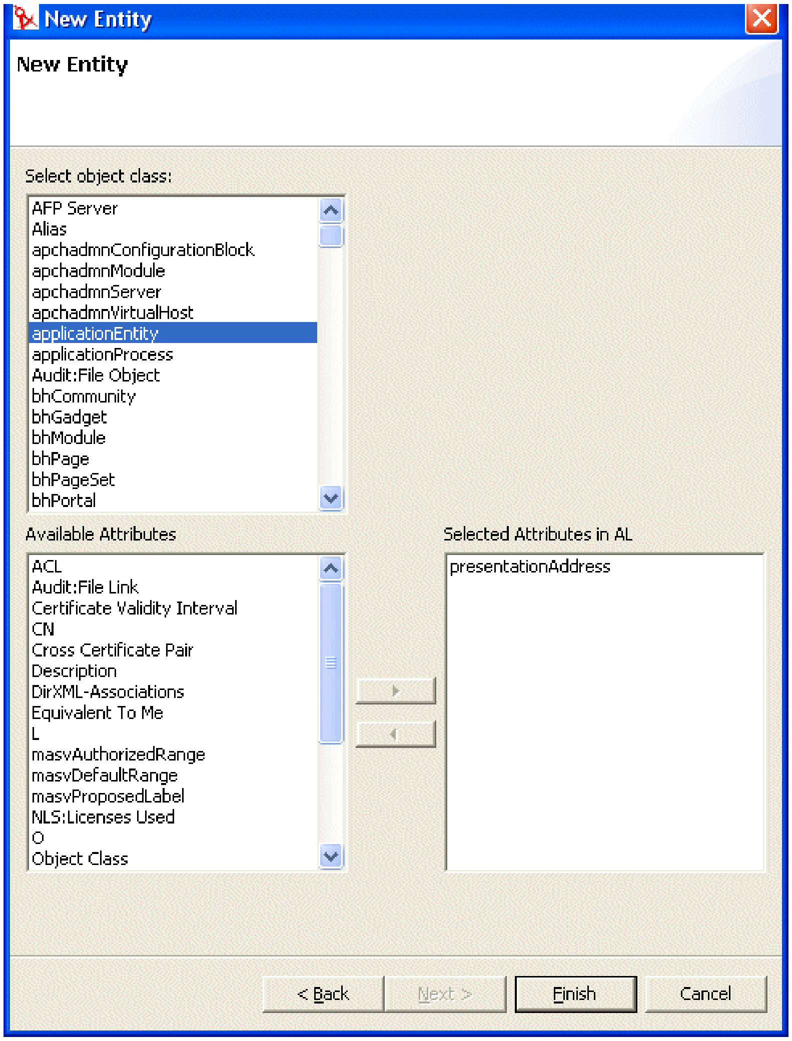
Observação: Se iniciar no menu Arquivo, a caixa de diálogo conterá campos não exibidos quando iniciada de uma das outras maneiras. Isso está indicado abaixo.



2 Preencha o painel da seguinte maneira:

Campo	Descrição
Projeto e Aplicativo de Aprovisionamento do Identity Manager	Selecione o projeto e o aplicativo de aprovisionamento do Identity Manager onde você deseja adicionar a entidade e os atributos. **Observação:** Estes campos só são exibidos quando você inicia o assistente pelo menu Arquivo.
Chave da Entidade	O identificador exclusivo da identidade.
Exibir Etiqueta	A string exibida sempre que a entidade é referenciada na interface do usuário.

3 Clique em *Avançar*. A caixa de diálogo Nova Entidade é exibida:



4 Escolha a classe de objeto da entidade a ser criada e selecione os atributos desejados na lista de atributos disponíveis.

Dica: Se a classe de objeto da entidade não estiver na lista Classes de Objeto Disponíveis, talvez seja preciso atualizar o arquivo de esquema local do Designer. Siga estas etapas descritas em "Para atualizar a lista de elementos de esquema disponíveis:" na página 89.

---

5 Clique em *Concluir*.

A folha de propriedades é exibida para edição.

Para obter mais informações, consulte "Referência de propriedade da entidade" na página 94.

Observação: Para que o atributo fique disponível para o aplicativo de usuário, distribua a entidade que o contém.

Adicionando atributos

Para adicionar um atributo:

1 Selecione uma entidade.

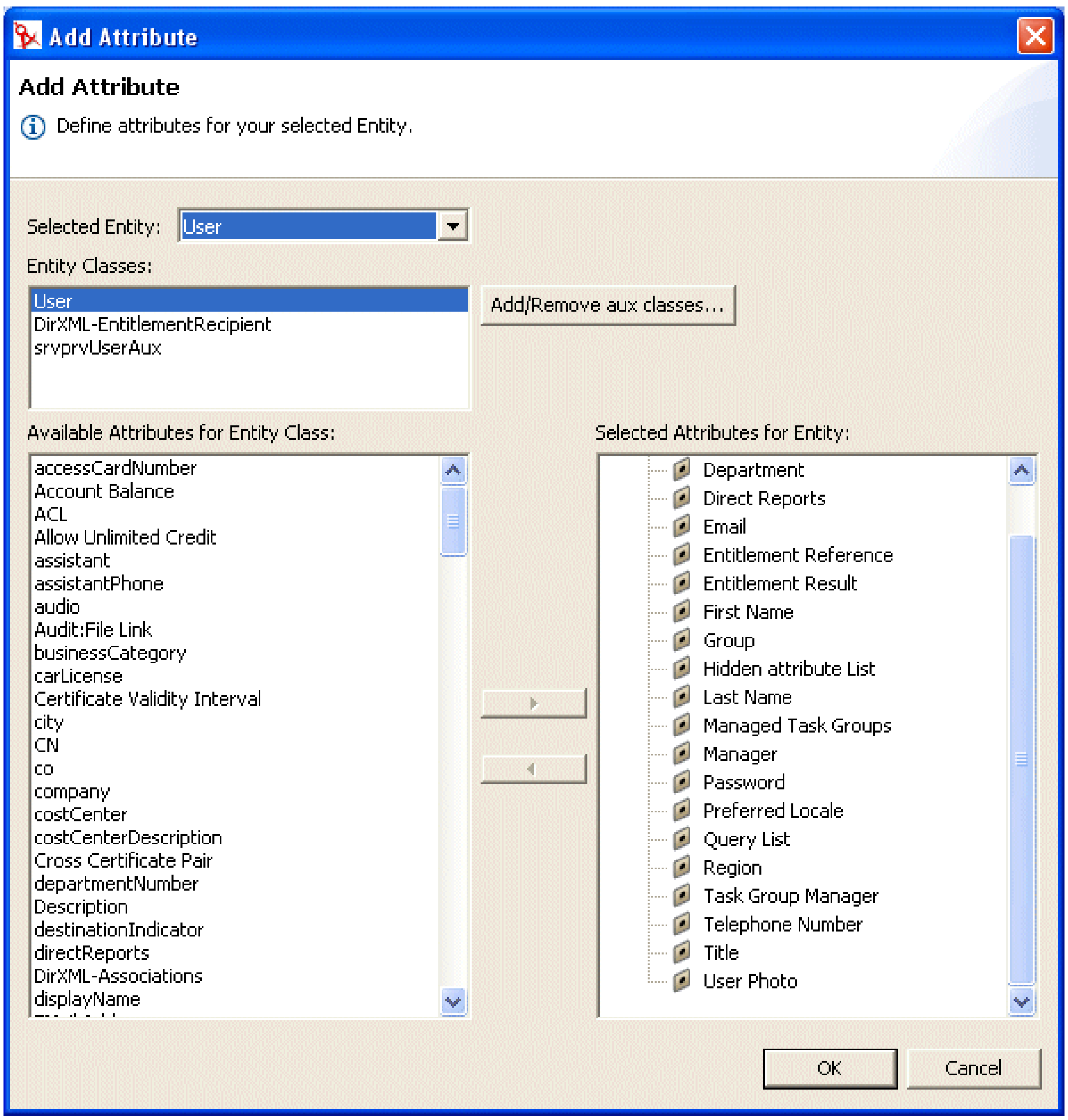
2 Adicione um atributo da seguinte maneira:

- Clique o botão direito do mouse e selecione *Adicionar Atributo*.

ou

- Clique no ícone *Adicionar Atributo*.

Você deverá informar o seguinte:



3 Escolha o atributo na lista *Atributos Disponíveis para Classe de Entidade* e adicione-o à lista *Atributos Selecionados para Entidade*.

Dica: Se o atributo a ser criado não estiver na lista Atributos Disponíveis para Classe de Entidade, talvez seja preciso atualizar o arquivo de esquema local do Designer. Siga estas etapas descritas em "Para atualizar a lista de elementos de esquema disponíveis:" na página 89.

4 Clique em *OK*.

A folha de propriedades é exibida para edição.

Para obter mais informações, consulte "Referência de propriedade do atributo" na página 97.

Observação: Para que o atributo fique disponível para o aplicativo de usuário, é preciso distribuí-lo.

Referência de propriedade da entidade

Você pode definir os seguintes tipos de propriedades nas entidades:

- "Propriedades de acesso da entidade" na página 94
- "Propriedades obrigatórias da entidade" na página 94
- "Propriedades de pesquisa da entidade" na página 95
- "Propriedades de criação e edição da entidade" na página 96
- "Propriedades do gerenciamento de senhas" na página 96

Propriedades de acesso da entidade

As *Propriedades de Acesso* controlam a maneira como o aplicativo de usuário interage com a entidade. Estão incluídas:

Propriedade	Descrição
Criar	**Marcada** — Este objeto pode ser criado pelo aplicativo de usuário.
Editar	**Desmarcada** — Este objeto não pode ser mudado pelo aplicativo de usuário, seja qual for a ACL subjacente.
	Marcada — Este objeto pode ser mudado, mas as ACLs do cofre de identidade são usadas para determinar isso.
Exibir	**Marcada** — Este objeto pode ser exibido pelo aplicativo de usuário.
Remover	**Marcada** — Este objeto pode ser apagado pelo aplicativo de usuário.

Propriedades obrigatórias da entidade

As propriedades *obrigatórias* da entidade são:

Nome da propriedade	Descrição
Chave	O identificador exclusivo da entidade. Ele define a maneira como o aplicativo de usuário fará referência ao objeto.
Exibir Etiqueta	Define como o objeto aparece na interface de usuário.
Nome de classe	O nome de classe do NDS (Novell Directory Service).

Nome da propriedade	Descrição
Nome LDAP	Nome de classe do objeto LDAP.
Pesquisar	**Marcada** — A entidade é pesquisável. As entidades usadas em consultas por portlets de identidade (como Lista de Pesquisa de Entidade ou Organograma da Entidade) devem ser selecionadas (verdadeiro).
Classes Auxiliares	Uma lista de zero ou mais classes auxiliares para a entidade. Se adicionar classes auxiliares, você precisará especificar o nome LDAP e o nome NDS da classe auxiliar, e indicar se ela pode ser pesquisada.

Propriedades de pesquisa da entidade

As *propriedades de Pesquisa da entidade* são:

Nome da propriedade	Descrição
Container de pesquisa	O nome exclusivo do container ou nó do LDAP onde a pesquisa começa (a raiz da pesquisa). Por exemplo: `ou=sample,o=ourOrg` Você pode percorrer o cofre de identidade para selecionar o container ou usar um dos parâmetros predefinidos descritos em "Usando parâmetros predefinidos" na página 97.
Escopo de pesquisa	Especifica onde a pesquisa ocorre em relação à raiz. Os valores são: **<Padrão>** — O escopo desta pesquisa equivale à seleção de containers e subcontainers. **Container** — A pesquisa ocorre no DN da raiz da pesquisa e todas as entradas no nível da raiz da pesquisa. **Container e subcontainers** — A pesquisa ocorre no DN da raiz da pesquisa e em todos os subcontainers. Equivale à seleção de **<Padrão>.** **Objeto** — Limita a pesquisa ao objeto especificado. Esta pesquisa é usada para verificar a existência do objeto especificado.
Limite de Tempo de Pesquisa [ms]	Especifique um valor em milissegundos ou especifique 0 para não ter limite de tempo.

Nome da propriedade	Descrição
Máximo de Entradas da Pesquisa	Especifique o número máximo de entradas de resultado a serem retornadas para uma pesquisa. Especifique 0 se quiser usar a configuração de tempo de execução. Recomendações: Defina **entre 100 e 200** para maior eficiência **Não** defina um valor superior a 1000

Propriedades de criação e edição da entidade

As *propriedades de criação e edição da entidade* são:

Nome da propriedade	Definição
Criar Container	O nome do container onde uma nova entidade deste tipo é criada. Você pode percorrer o cofre de identidade para selecionar o container ou usar um dos parâmetros predefinidos descritos em "Usando parâmetros predefinidos" na página 97. Se esse valor não for especificado, o portlet Criar solicitará que o usuário especifique um container para o novo objeto. O portlet usará a raiz da pesquisa especificada na definição de entidade como a base e permitirá que o usuário detalhe a partir daí. Se nenhuma raiz da pesquisa estiver especificada na definição de entidade, ele usará o DN da raiz especificado durante a instalação do aplicativo de usuário.
Atributo de Nomeação	O atributo de nomeação da entidade – o RDN (Relative Distinguished Name – Nome Exclusivo Relativo). Esse valor só é necessário para as entidades em que o parâmetro de acesso Criar é selecionado.
Alternar Entidade de Edição	Os atributos da entidade de edição são exibidos no modo de edição do portlet Detalhes. Escolha uma entidade na lista suspensa ou <Nenhum> se o portlet Detalhes não exibir a entidade.

Propriedades do gerenciamento de senhas

As *propriedades do gerenciamento de senhas* são:

Nome da propriedade	Definição
Atributo de Senha	Escolha o atributo onde a senha da entidade será armazenada.
Senha obrigatória quando atributo é criado	**Marcada** — Uma senha é exigida quando a entidade é criada.

Usando parâmetros predefinidos

O editor da camada de abstração do diretório permite que você use parâmetros predefinidos para certos valores. Os parâmetros são:

Parâmetro predefinido	Descrição
%driver-root%	Representa o DN do Driver de Aprovisionamento. Esse valor é especificado durante a configuração do aplicativo de usuário no momento da instalação ou em uma configuração posterior. Ele é armazenado na configuração do domínio do aplicativo de usuário.
%user-root%	Representa o DN do Container de Usuário. Esse valor é especificado durante a configuração do aplicativo de usuário no momento da instalação ou em uma configuração posterior. Ele é armazenado na configuração do domínio do aplicativo de usuário.
%group-root%	Representa o DN do Container de Grupo. Esse valor é especificado durante a configuração do aplicativo de usuário no momento da instalação ou em uma configuração posterior. Ele é armazenado na configuração do domínio do aplicativo de usuário.

Referência de propriedade do atributo

Você pode definir os seguintes tipos de propriedades nos atributos:

- "Propriedades de acesso do atributo" na página 97
- "Propriedades obrigatórias do atributo" na página 98
- "Propriedades de filtro e formatação do atributo" na página 99
- "Propriedades de controle de IU do atributo" na página 99

Propriedades de acesso do atributo

As *propriedades de acesso do atributo* são:

Nome	Descrição
Editar	**Marcada** — Este atributo pode ser editado/modificado pelo aplicativo de usuário. Mesmo com a propriedade selecionada (verdadeiro), o atributo pode continuar não editável se os direitos efetivos das ACLs subjacentes do cofre de identidade impedirem a edição.
Habilitar	**Desmarcada** — Este atributo não pode ser usado pelo aplicativo de usuário. Essa ação é semelhante a remover a entrada do arquivo.

Nome	Descrição
Ocultar	Controla se a caixa de seleção Ocultar do aplicativo de usuário está habilitada ou desabilitada. A caixa de seleção Ocultar permite que os usuários controlem se um atributo (por exemplo, suas fotos) será exibido pelo aplicativo. **Desmarcada** — A caixa de seleção Ocultar está desabilitada para o atributo, de forma que o usuário não pode optar por ocultar o atributo. **Marcada** — A caixa de seleção Ocultar pode ser habilitada no aplicativo de usuário. Entretanto, é preciso que as seguintes informações sobre o usuário conectado também sejam verdadeiras. Ele: ◆ É o proprietário do atributo ou um Administrador de Aplicativo de Usuário. ◆ Tem direitos de Trustee para atualizar o atributo srvprvHideAttributes no cofre de identidade. Se esses requisitos não forem atendidos, a caixa de seleção Ocultar será desabilitada na interface de usuário mesmo que esteja marcada (verdadeiro). **Dica:** Quando um usuário oculta um atributo que contém uma imagem, os usuários que visualizaram a imagem continuarão a visualizá-la até o cache de seus browsers ser atualizado.
Vários valores	Especifica se o atributo pode ter vários valores; por exemplo, um número de telefone. **Marcada** — O atributo pode ter vários valores.
Ler	**Marcada** — O aplicativo de usuário pode consultar esse atributo. Para a maioria dos atributos, esta propriedade deve ser selecionada (verdadeiro); porém, para alguns atributos, como as senhas, ela deve ser desmarcada.
Obrigatório	**Marcada** — O atributo pode ser especificado.
Pesquisar	**Marcada** — O aplicativo de usuário pode pesquisar o atributo. Os atributos usados em consultas por portlets de identidade (como Lista de Pesquisa de Identidade ou Organograma da Entidade) devem ser selecionados. **Dica:** Se algum atributo usado em uma pesquisa também estiver indexado no eDirectory, a pesquisa será mais rápida.
Exibir	**Marcada** — O aplicativo de usuário pode exibir o atributo. Na maioria dos casos, esta propriedade é verdadeira; porém, para alguns atributos, como as senhas, ela provavelmente seria desmarcada.

Propriedades obrigatórias do atributo

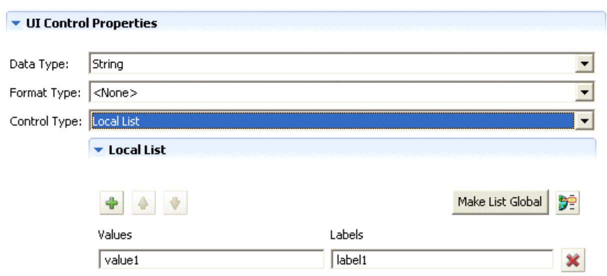
Nome	Descrição
Chave	O identificador exclusivo do atributo.
Exibir Etiqueta	A etiqueta exibida no aplicativo de usuário.
Nome do Atributo	O nome NDS do atributo.
Nome LDAP	O nome LDAP do atributo.

Propriedades de filtro e formatação do atributo

Nome	Descrição
Filtrar: atributo WHERE	Permite que você especifique um filtro LDAP na procura do cofre de identidade pelo atributo.
Habilitar	**Marcada** — Habilita o filtro.

Propriedades de controle de IU do atributo

Nome	Descrição
Tipo de Dados	Escolha um tipo de dados na seguinte lista: ◆ Binário ◆ Booleano ◆ DN ◆ Número Inteiro ◆ String Localizada ◆ String ◆ Horário
Tipo de Formato	Usada pelo aplicativo de usuário para formatar dados. Os tipos de formato incluem: ◆ Nenhum ◆ AOL IM ◆ E-mail ◆ Groupwise IM ◆ Imagem ◆ Telefone ◆ Yahoo IM ◆ URL de Imagem ◆ Data ◆ Data/Hora Os tipos de formato dependem do tipo dos dados. Por exemplo, dados do tipo Hora só podem ser associados a formatos Data e Data/Hora.

Nome	Descrição
Tipo de Controle	Os tipos incluem: **DNLookup** — Define que o atributo contém uma referência DN. Use-o para: ◆ Preencher uma lista com os resultados de uma pesquisa DN entre as entidades relacionadas ◆ Manter a integridade referencial entre atributos de referência DN durante atualizações e exclusões O aplicativo de usuário utiliza essas informações para gerar elementos especiais da interface de usuário e para otimizar pesquisas com base na definição de DNLookup. Para obter mais informações, consulte “Usando tipos de controle DNLookup” na página 100. **Lista Global** — Exibe o atributo como uma lista suspensa cujo conteúdo é definido em um arquivo fora da definição do atributo. Para obter mais informações, consulte a Seção 4.4, “Trabalhando com listas” na página 103. **Lista Local** — Exibe o atributo como uma lista suspensa cujo conteúdo é definido com o atributo. Para definir uma lista local: 1. Com o atributo selecionado, defina o tipo de controle como Lista Local.  2. Clique no botão Adicionar para adicionar mais valores. Use os botões de seta para cima e para baixo para mudar a posição do item na lista. Na coluna Valor, digite o valor a ser gravado no cofre de identidade. O nome só pode conter letras minúsculas, números e sublinhado (_). 3. Na coluna Etiquetas, digite o texto a ser exibido na interface de usuário. **Faixa** — Use o tipo de controle Faixa com os tipos de dados Número Inteiro para registrar entradas do usuário em uma faixa seqüencial de valores. Você fornecerá os valores inicial e final da faixa.

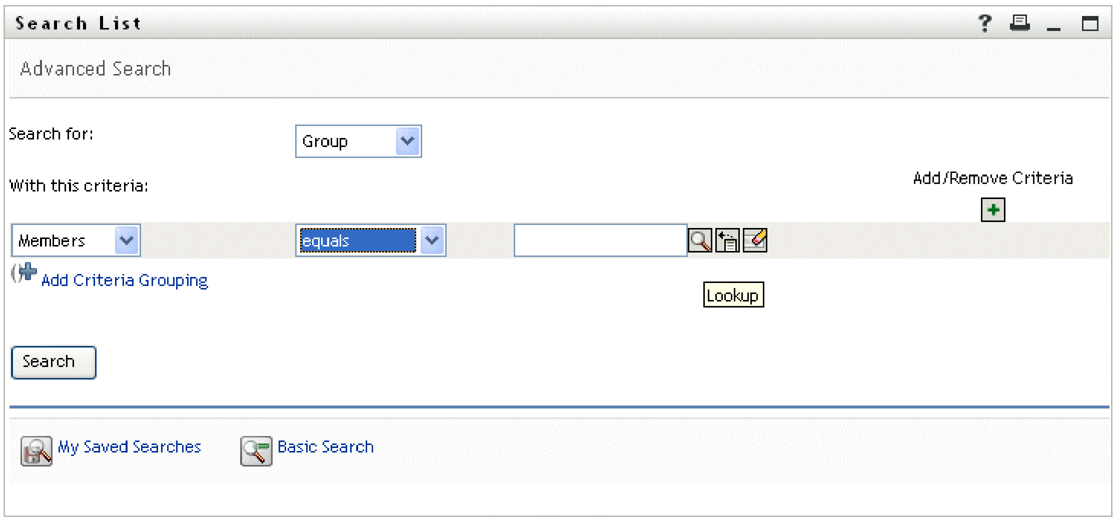
Usando tipos de controle DNLookup

Quando você define um tipo de controle como DNLookup, significa que:

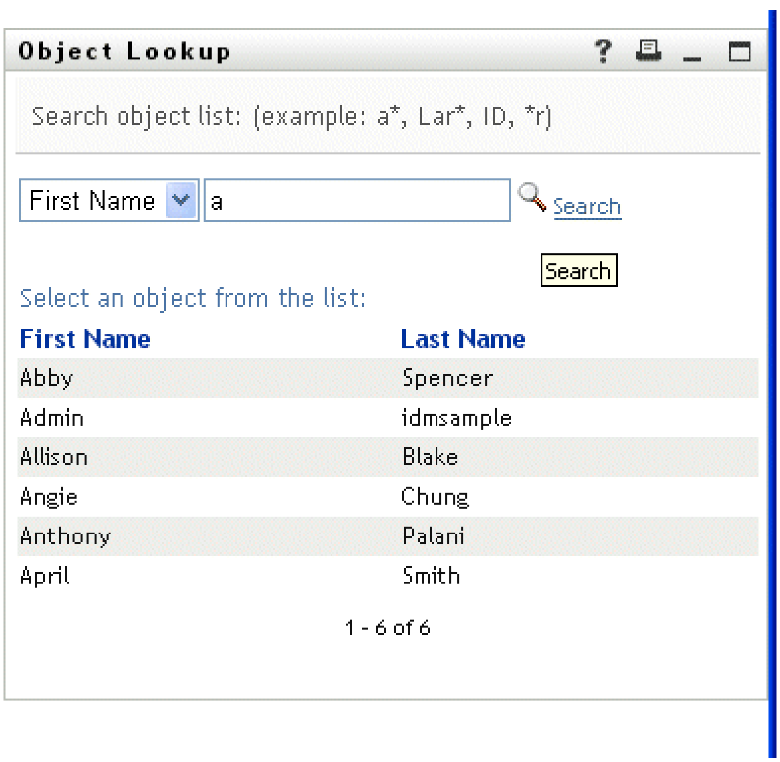
- Os usuários podem selecionar em uma lista de valores possíveis ao pesquisarem o atributo.
- Quando o atributo é criado, preenchido ou apagado, um atributo em uma entidade relacionada será atualizado corretamente de acordo com a ação do usuário (criar, apagar, atualizar) para manter a integridade referencial.

DNLookups para listas de seleção

O aplicativo de usuário instalado contém definições de entidade para Usuários e Grupos. A definição de entidade Usuários contém um atributo chamado Grupo que é definido como um tipo de controle DNLookup. Dessa forma, todo portlet de identidade pode fornecer uma lista de seleção de grupo para determinado usuário. Por exemplo, um usuário opta por fazer uma pesquisa de diretório. Ele quer encontrar um usuário em um grupo, mas não sabe o nome do grupo. Ele seleciona Usuário como o objeto de pesquisa e inclui Grupo como critério de pesquisa a ser indicado aqui.



Já que Grupo é definido como um tipo de controle DNLookup para a entidade Usuário, o ícone de Pesquisa é exibido. Se o usuário o selecionar, uma lista de grupos possíveis será exibida:



O usuário pode selecionar um grupo na lista.

DNLookups para integridade referencial

DNLookups para atualizações e sincronização são importantes porque o LDAP permite o mapeamento bidirecional de relacionamentos de grupo. Por exemplo, seus dados podem ser configurados para que:

- O objeto Usuário contenha um atributo de grupo. O atributo de grupo:
- Tem vários valores
- Lista todos os grupos aos quais um usuário pertence
- O objeto Grupo contenha um atributo de usuário. O atributo de usuário:
- Tem vários valores
- Lista todos os usuários que pertencem ao grupo

Isso significa que você precisa ter um atributo no objeto Usuário que mostre todos os grupos aos quais o usuário pertence, e no objeto Grupo, você tem um atributo DN que inclui todos os integrantes desse grupo.

Quando o usuário solicita uma atualização, o aplicativo de usuário deve manter os relacionamentos e garantir que os atributos de origem e de destino sejam sincronizados. Na DNLookup, você especificará os dois atributos que devem ser sincronizados. Você pode usar essa técnica para garantir a sincronização entre todos os objetos relacionados, e não somente os objetos estruturais do grupo. Para criar esse tipo de controle DNLookup, especifique as propriedades DNLookup avançadas descritas na referência *propriedades de integridade relacional DNLookup*.

Referência da propriedade DNLookup

As propriedades de exibição DNLookup são:

Campo	Definição
Entidade de Pesquisa	O nome da entidade da pesquisa. Por exemplo, a entidade Grupo de Tarefas contém um atributo para Gerenciador de Tarefas. Para preencher esse campo, você precisa saber quais usuários são Gerenciadores de Tarefas.
Entidade de detalhe	A chave da entidade cujos detalhes você deseja exibir se o usuário solicitar mais informações ao clicar em um link de hipertexto no aplicativo de usuário. Quando você define uma DNLookup, os portlets de identidade podem oferecer um link de hipertexto que permite aos usuários exibir os detalhes do objeto vinculado.
Atributos a exibir	Escolha um ou mais atributos a serem exibidos quando a pesquisa estiver concluída.

Campo	Definição
Executar Consulta Automática	Define como o campo **Atributos a exibir** (acima) será exibido. ◆ **Marcada** — Realiza uma consulta automática da entidade e apresenta os resultados em uma lista selecionável. Não convém escolher essa opção se o número de dados retornados for muito alto, pois isso forçará o usuário a percorrer um conjunto grande de resultados. ◆ **Desmarcada** — Permite que o usuário especifique os critérios de pesquisa para a consulta da entidade e apresenta os resultados em uma lista selecionável.

Propriedades de integridade relacional DNLookup — Estas propriedades são usadas para sincronizar dados entre dois objetos, como grupos e membros de grupos.

Propriedade	Definição
Atributos de origem a atualizar	Nome do atributo a ser atualizado. O atributo deve conter uma referência DN para **Atributos de destino a atualizar**. Isso é necessário para sincronizar atributos em dois objetos diferentes.
Atributos de destino a atualizar	Nome do atributo que deve ser atualizado junto com **Atributos de origem a atualizar**. É um nome do atributo LDAP. Necessário para sincronizar atributos em dois objetos distintos. O atributo deve conter uma referência DN.
Classes auxiliares de destino, se houver	Nome da classe auxiliar que contém os **Atributos de destino a atualizar**.

4.4 Trabalhando com listas

O nó de listas permite definir o conteúdo de listas globais. As listas globais são usadas pelo aplicativo de usuário do Identity Manager para.

- Fornecer uma lista de valores de um atributo. Quando o atributo é exibido para edição na interface de usuário, os valores possíveis aparecem como uma lista suspensa.
- Elas são usadas para definir categorias disponíveis para o plug-in Provisioning Request Configuration do iManager. Essa é uma lista especial. Para obter detalhes, consulte a Seção 4.4.2, “Sobre a lista Categoria de Aprovisionamento” na página 105.

Para criar uma nova lista global

1 Inicie o Assistente de Nova Lista de uma das seguintes maneiras:

   No *modo de aprovisionamento*:

   - Selecione *Arquivo>Novo>Aprovisionamento*. Escolha *Lista de Camadas de Abstração do Diretório*. Clique em *Avançar*.
   - Selecione o nó *Listas*, clique o botão direito do mouse e escolha *Novo*.

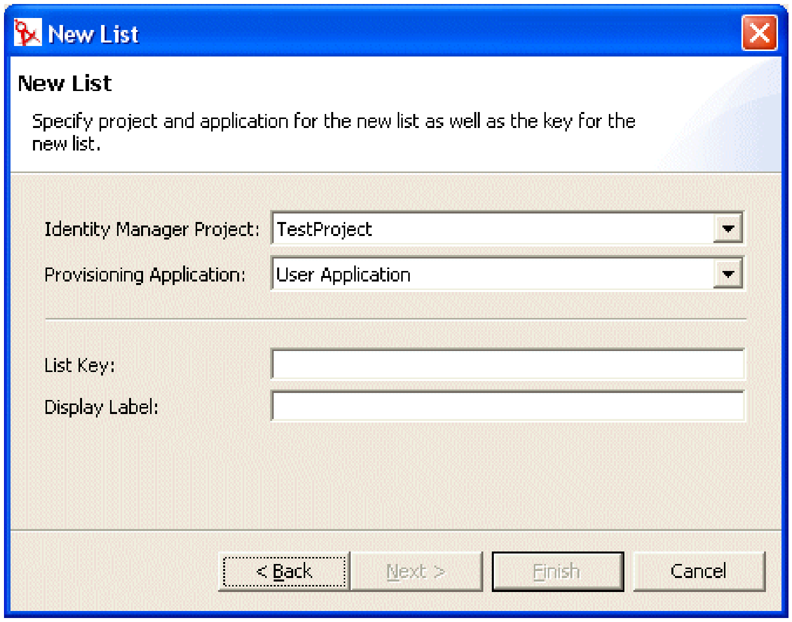
   No *editor da camada de abstração do diretório*:

   - Clique no botão *Nova Lista*.

- Selecione o nó Listas, clique o botão direito do mouse e escolha *Adicionar Lista*.

A caixa de diálogo Nova Lista é exibida.

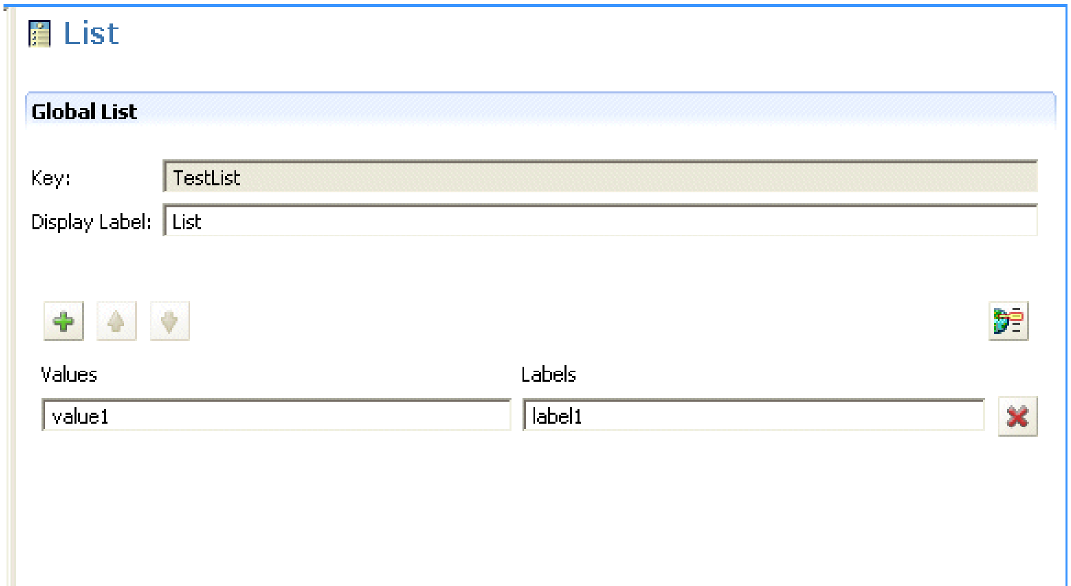
Observação: Se iniciada pelo menu Arquivo, a caixa de diálogo conterá campos não exibidos quando iniciada de uma das outras maneiras.



2 Preencha o painel da seguinte maneira:

Campo	Descrição
Projeto e aplicativo de aprovisionamento do Identity Manager	Selecione o projeto e o aplicativo de aprovisionamento do Identity Manager onde você deseja adicionar a entidade e os atributos. **Observação:** Estes campos só são exibidos quando você inicia o assistente pelo menu Arquivo.
Chave da Lista	O identificador exclusivo da lista.
Exibir Etiqueta	A string usada sempre que a lista é referenciada na interface do usuário.

3 Clique em *Concluir*. A folha de propriedades Listas Globais é exibida.



4 Preencha estes campos:

Campo	**Descrição**
Exibir Etiqueta	O nome da lista como ele aparece no Designer.
Etiquetas	O texto do item da lista a ser exibido na interface de usuário.
Valores	O valor do item da lista a ser armazenado no cofre de identidade. O nome só pode conter letras minúsculas, números e sublinhado (_).

Agora a lista está disponível no ambiente de design.

5 Grave o projeto.

Observação: Para que a lista fique disponível para o ambiente em tempo de execução, é preciso distribuí-la.

4.4.1 Sobre a lista Local Preferido

A lista Local Preferido representa o idioma padrão que será usado caso o idioma do browser não seja um dos idiomas aceitos. O conteúdo desta lista será exibido pela configuração padrão da ação Editar Usuário no aplicativo de usuário.

4.4.2 Sobre a lista Categoria de Aprovisionamento

A lista Categoria de Aprovisionamento define o conjunto de categorias que o ajudam a organizar Recursos Aprovisionados (Direitos) e Solicitações de Aprovisionamento. As categorias dessa lista são exibidas em:

- *iManager* — Plug-in Configuração da Solicitação de Aprovisionamento

* *Aplicativo de usuário* — Guia Solicitações e Aprovações

Não é possível mudar a chave da lista Solicitação de Aprovisionamento, mas você pode incluir mais itens na lista ou mudar os valores e as etiquetas da categoria existente.

Para modificar o conteúdo da lista Categoria de Aprovisionamento:

1. Verifique se o projeto correto está aberto no editor.
2. Clique no nó Listas.
3. Selecione *Categoria de Aprovisionamento*.
4. Use o painel de propriedades da lista global para efetuar as modificações.

   Observação: O campo Valores é usado para preencher a chave da categoria. O campo Valores está restrito a letras minúsculas, números e sublinhados (_), pois esses são os únicos caracteres válidos na chave da categoria. A chave da categoria é usada internamente como um modificador da categoria.

5. Grave e distribua suas mudanças. Lembre-se de atualizar o cache do servidor de aplicativos.

   Depois de distribuídas, as mudanças são refletidas no aplicativo de usuário e no plug-in iManager.

4.5 Trabalhando com relacionamentos de Organograma

O nó de relacionamentos de organograma permite que você defina relacionamentos hierárquicos entre as entidades definidas na camada de abstração do diretório. O relacionamento pode ser entre entidades semelhantes (como usuário /usuário) ou não (como usuário/dispositivo).

Os seguintes relacionamentos são definidos para o aplicativo de usuário:

* Participação no grupo
* Gerentes e Funcionários
* Grupos de usuários

Para distribuir um relacionamento corretamente, todos os componentes (entidades e atributos) do relacionamento já devem ter sido distribuídos.

Para criar um novo relacionamento:

1. Você pode criar um novo relacionamento em qualquer destas maneiras:

   No *modo de aprovisionamento*:

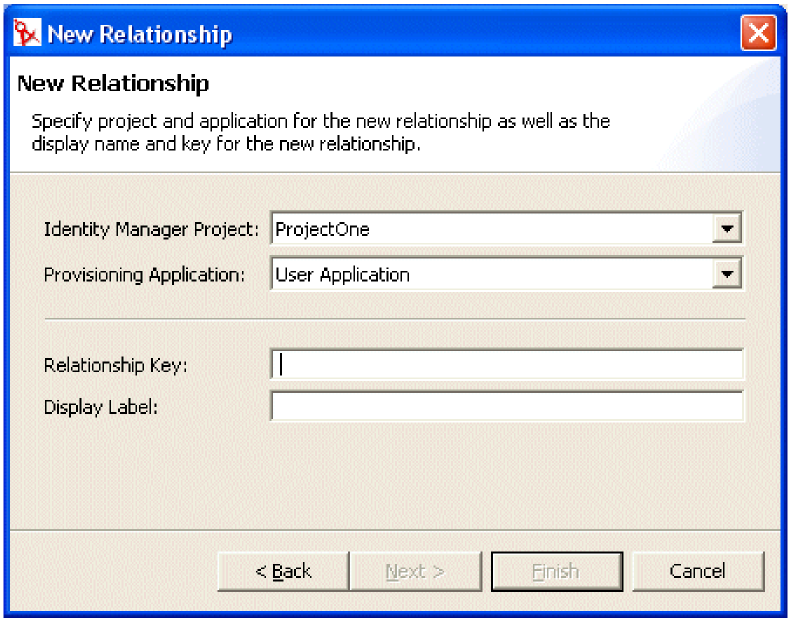
   * Selecione *Arquivo>Novo>Aprovisionamento*. Escolha *Relacionamento da Camada de Abstração do Diretório* e clique em *Avançar*.
   * Clique o botão direito do mouse e selecione o nó *Relacionamentos de Organograma*, e escolha *Adicionar*.

   No *editor da camada de abstração do diretório*:

   * Clique no botão *Adicionar Relacionamento*.
   * Clique o botão direito do mouse e selecione o nó *Relacionamentos de Organograma*, e escolha *Adicionar Relacionamento*.

A caixa de diálogo Novo Relacionamento é exibida.

Observação: Quando iniciada pelo menu Arquivo, a caixa de diálogo conterá campos não exibidos quando iniciada de uma das outras maneiras.

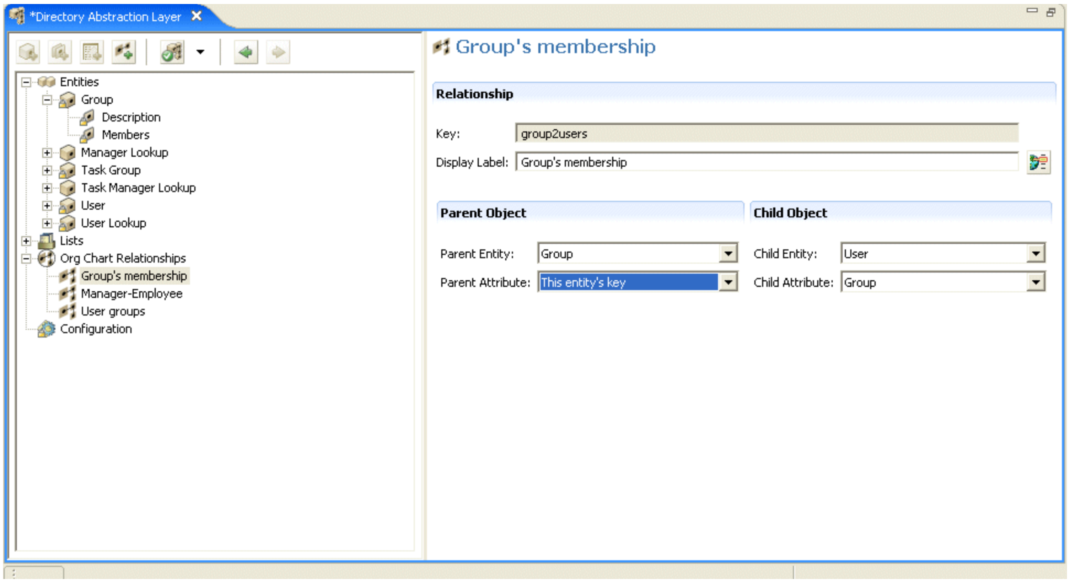


2 Preencha o painel da seguinte maneira:

Campo	O que fazer
Projeto e Aplicativo de Aprovisionamento do Identity Manager	Verifique se o projeto e os aplicativos de aprovisionamento corretos do Identity Manager estão selecionados. **Observação:** Este campo indica quando você cria relacionamentos no menu Arquivo.
Chave de Relacionamento	Digite um valor exclusivo para a chave de relacionamento.
Exibir Etiqueta	Digite a string que será exibida toda vez que os relacionamentos aparecerem na interface de usuário do Identity Manager.

3 Clique em *Concluir*.

O relacionamento é criado e sua folha de propriedades é aberta para edição.



4.5.1 Referência das propriedades de relacionamento

Campo	Descrição
Chave	O identificador exclusivo apenas leitura para o relacionamento. **Dica:** Você especificará este valor na folha de preferências do portlet Organograma.
Exibir Etiqueta	Especifique um nome a ser exibido quando outros portlets de identidade fizerem referência ao relacionamento. Por exemplo, esse valor é exibido quando os usuários clicam no ícone Escolher Organograma no portlet Detalhes. Clique em **Localizar** para fornecer a tradução do texto da etiqueta de exibição.
Entidade pai	Escolha uma entidade na lista suspensa. A entidade escolhida será o objeto pai na hierarquia de organogramas. Por exemplo, em um relacionamento entre Gerentes e Funcionários, a Entidade Pai seria Usuário. Em um relacionamento entre Grupo e Membros, a Entidade Pai seria Grupo. **Requisitos da camada de abstração do diretório** — As entidades desta lista são um subconjunto das entidades definidas na camada de abstração do diretório. As entidades pai devem ter a propriedade de ver acesso selecionada (verdadeiro).

Campo	Descrição
Atributo pai	Escolha um atributo na lista suspensa. Este atributo é usado para localizar entidades filho correspondentes. Quando o valor deste atributo tem um correspondente em um atributo da entidade filho (veja Atributo filho abaixo), pode-se estabelecer um relacionamento. **Requisitos da camada de abstração do diretório** — Esta lista de atributos é preenchida com os atributos da entidade pai selecionada. Ela inclui somente os atributos definidos como tipo de controle DNLookup
Entidade filho	Escolha a entidade que será o objeto filho na hierarquia. Por exemplo, em um relacionamento entre Gerentes e Funcionários, seria usuário. Em um relacionamento entre Funcionários e Recursos, seria Dispositivos. Essa entidade deve conter o atributo que está relacionado ao atributo Pai.
Atributo filho	Escolha o atributo que melhor corresponde ao atributo pai. Esta opção especifica o atributo na entidade filho que será usado para localizar entidades pai correspondentes. Quando o valor deste atributo tem um correspondente em um atributo da entidade pai (veja Atributo pai acima), pode-se estabelecer um relacionamento.

Observação: Grupos dinâmicos não têm suporte integral do portlet Organograma. Não é possível definir um grupo dinâmico como a entidade pai de um relacionamento, mas você pode definir um grupo dinâmico como a entidade filho de um relacionamento.

Para apagar um relacionamento:

1 Selecione o relacionamento que você deseja apagar.

2 Clique o botão direito do mouse e escolha *Apagar*.

4.6 Trabalhando com definições de configuração

O nó Configuração permite que você defina propriedades de configuração geral para o aplicativo de usuário. Estão incluídas:

Propriedade	Descrição
Entidade ‘Meu Perfil’ Padrão	Define a entidade a ser exibida quando o usuário clica em **Meu Perfil** na interface de usuário. Este campo mostra apenas as entidades cuja classe de objeto é usuário (ou LDAP inetOrgPerson).
Locale Padrão	Define o idioma padrão que será usado para as etiquetas de exibição no aplicativo de usuário. Se o browser não estiver definido para um idioma sem suporte, este será o locale usado. **Observação:** O locale do browser substituirá o locale padrão dos idiomas suportados.

Propriedade	Descrição
Classes de Container	Informa a ação de Criar Usuário ou Grupo com o conteúdo de uma lista de seleção das classes de container. O usuário escolhe um container na lista de seleção como a localização para o objeto recém-criado.

4.7 Localizando texto de exibição

O editor da camada de abstração do diretório facilita a localização do texto de exibição para:

- Etiquetas de exibição de entidades e atributos
- Nomes de relacionamentos de organogramas
- Itens de listas globais e locais

4.7.1 Idiomas suportados

O texto de exibição pode estar em um ou mais destes idiomas:

- Inglês
- Francês
- Alemão
- Italiano
- Japonês
- Coreano
- Português
- Russo
- Chinês Simplificado
- Espanhol
- Chinês Tradicional

4.7.2 Localizando texto

O editor da camada de abstração do diretório oferece diversos meios para localizar as definições da camada de abstração. Estes são os meios de acesso às caixas de diálogo de localização:

Para definir o texto de localização de	Ação
Todo item localizável na camada de abstração do diretório	◆ Clique em **Definir Localização Global (**na barra de ferramentas do editor da camada de abstração do diretório). Selecione o idioma de destino antes de inserir texto no campo de destino.

Para definir o texto de localização de	Ação
Uma entidade, um relacionamento ou uma lista específicos	◆ Na tela de árvore do editor da camada de abstração do diretório, selecione o objeto a ser localizado. ◆ Clique o botão direito do mouse e selecione **Localizar**. Selecione o idioma de destino antes de inserir texto no campo de destino.
Uma única etiqueta de exibição	◆ Selecione uma entidade ou um atributo específico. ◆ Clique em **Localizar Etiqueta de Exibição** (ao lado do campo Exibir Etiqueta no painel de propriedades).

A aparência das caixas de diálogo pode diferir um pouco, mas elas contêm estes campos:

- *Origem* — Normalmente é o tipo de objeto (entidade, lista ou relacionamento) e a chave
- *Fonte* — O texto a ser traduzido (etiqueta de exibição)
- *Idioma de Destino* — Um dos idiomas suportados
- *Destino* — O texto da tradução

4.8 Importando, validando e distribuindo definições da camada de abstração do diretório

Importação, validação e distribuição das definições da camada de abstração do diretório são ações realizadas no modo de aprovisionamento do Designer.

- Seção 4.8.1, "Sobre como importar" na página 111
- Seção 4.8.2, "Sobre a validação" na página 114
- Seção 4.8.3, "Sobre a distribuição" na página 114

4.8.1 Sobre como importar

O recurso de importação permite que você importe um conjunto de definições. Convém usá-lo quando:

- Iniciar um novo projeto com base em um projeto distribuído.
- Compartilhar definições com outros desenvolvedores que trabalham no mesmo projeto. Por exemplo, o outro desenvolvedor adiciona um atributo à entidade de usuário ou uma nova lista global. Se o desenvolvedor distribui a nova definição para o cofre de identidade, você poderá importá-la e assim vocês dois trabalharão com definições idênticas.

Para importar definições:

1. Abra o *modo de aprovisionamento*.
2. Determine se deseja importar:
   - Um conjunto completo de definições
   - Um conjunto de um tipo de definição, como todas as entidades ou todos os relacionamentos.
   - Um objeto específico (como a entidade de usuário)

3 Para importar:

- Um objeto específico, selecione-o na lista, clique o botão direito do mouse e selecione *Importar Objeto*.
- Um conjunto completo de definições, selecione o nó da Camada de Abstração do Diretório, clique o botão direito do mouse e selecione *Importar Tudo* ou *Importar Objeto*.

4 Clique no ícone de pesquisa do eDirectory e navegue até o nó do Modelo de Diretório e selecione os objetos para a importação e, em seguida, clique em *OK*.

- Se houver uma correspondência entre os objetos, você será notificado de que não há diferenças e que a importação não prosseguirá.
- Se não houver correspondência, você poderá confirmar quais objetos serão importados. Verifique os itens selecionados para importação, efetue as mudanças necessárias e clique em *OK*.

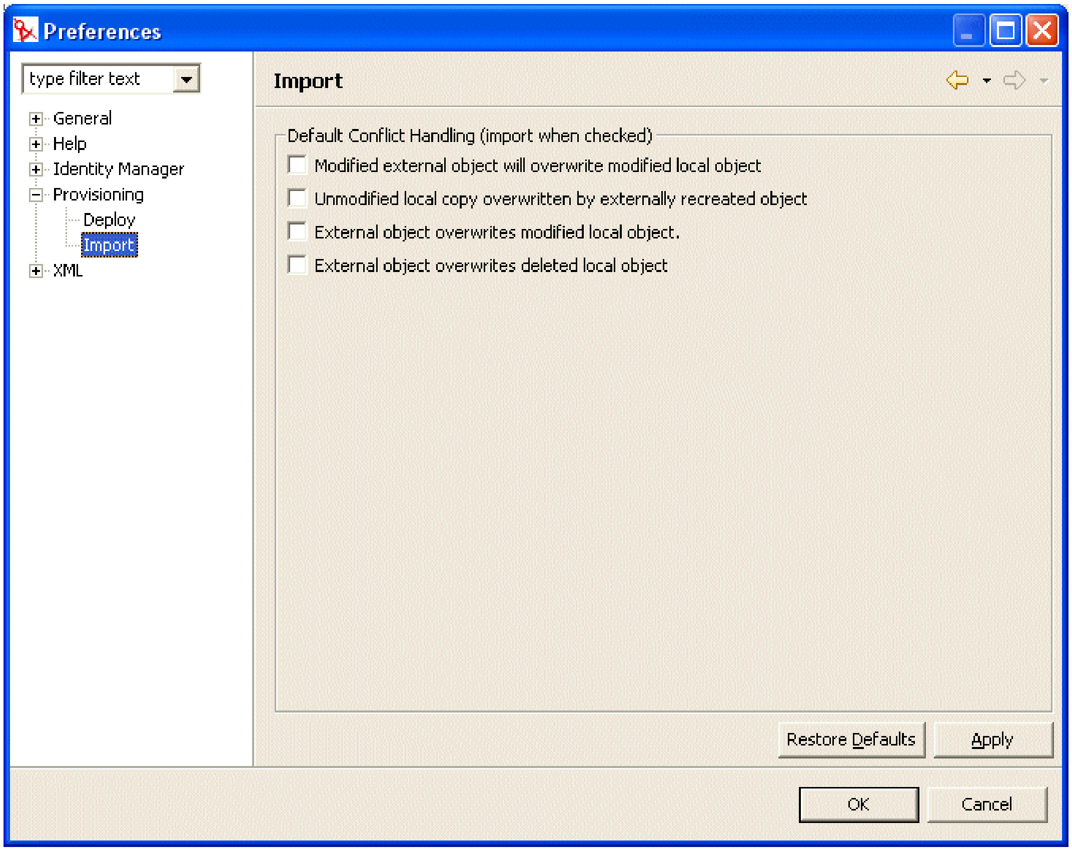
Definindo preferências de importação

As preferências de importação permitem que você especifique como deseja que o Designer solucione conflitos entre os dados no cofre de identidade e os arquivos da camada de abstração do diretório local. Esses conflitos podem surgir devido ao acesso de diferentes usuários e ferramentas às definições da camada de abstração do diretório do cofre de identidade. As definições podem ser mudadas por outros administradores ou desenvolvedores com o uso de ferramentas do iManager ou projeto com base em seu próprio Designer. Se ocorrerem conflitos entre as definições no seu sistema de arquivos local e o cofre de identidade, essas preferências permitirão que você especifique como os conflitos serão tratados.

Para definir preferências de importação:

1 Escolha *Janela>Preferências*.

2 Abra o nó de aprovisionamento da árvore e clique em *Importar*.



3 Escolha as preferências.

Preferência	Descrição
Objeto externo modificado sobregravará objeto local modificado	As definições do arquivo local e do cofre de identidade contêm mudanças. As mudanças locais ainda não foram distribuídas. Selecione esta opção se quiser que o objeto do cofre de identidade sobregrave as mudanças efetuadas no arquivo local.
Cópia local não modificada sobregravada por objeto recriado externamente	O objeto do cofre de identidade foi apagado e depois recriado. O conjunto de arquivos locais inclui a definição original sem mudanças. Selecione esta opção se quiser que a importação sobregrave a cópia local.
Objeto externo sobregrava objeto local modificado	O arquivo local contém mudanças não distribuídas no cofre de identidade. Selecione esta opção se quiser que os arquivos locais sejam sobregravados durante a importação.

Preferência	Descrição
Objeto externo sobregrava objeto local apagado	Você apagou uma definição localmente mas não distribuiu as mudanças. Isso significa que o objeto permanece no cofre de identidade. Selecione esta opção se quiser que os objetos do cofre de identidade sejam copiados para o sistema de arquivos local. Se você escolher esta opção, perderá as mudanças não distribuídas.

4.8.2 Sobre a validação

Você pode validar as definições de dados da camada de abstração do diretório no sistema de arquivos local antes de tentar distribuí-las. A validação:

- Verifica se o código XML está bem composto e compatível com o esquema que define os elementos necessários a entidades, atributos, listas, relacionamentos e outros itens.
- Verifica em cada entidade se as referências a outras entidades e listas globais são válidas.

Por exemplo, ao validar uma entidade e seus atributos, o validador verifica se todas as referências a outras entidades feitas pelos campos *Entidade de Edição*, *DN Lookup* e *Entidade de Detalhe* fazem referência a entidades que realmente existem.

- Verifica se cada entidade tem ao menos um atributo definido.
- Garante que toda lista local e global contenha no mínimo um item.

Você valida definições seletivamente no *modo de aprovisionamento*. Para validar:

- Todos os itens de um nó, selecione o nó, clique o botão direito do mouse e selecione *Validar*.
- Um único objeto em um nó, selecione o objeto, clique o botão direito do mouse e selecione *Validar*.

Para validar todas as definições, clique no botão *Validar Camada de Abstração* na barra de ferramentas da camada de abstração do diretório.

Observação: A validação não verifica a existência de objetos no cofre de identidade.

4.8.3 Sobre a distribuição

Você deve distribuir suas definições em um cofre de identidade para ver as mudanças resultantes no aplicativo de usuário do Identity Manager.

Para distribuir um conjunto de definições em um cofre de identidade:

1. Grave todas as mudanças efetuadas com o editor da camada de abstração do diretório.

   Se você não gravar suas mudanças antes de tentar a distribuição, o editor exibirá uma caixa de diálogo com as definições que não foram gravadas. Você será solicitado a gravar as mudanças mais recentes. Caso você não grave as mudanças, o objeto será distribuído no servidor sem as mudanças que não foram gravadas. O fato de você não gravar as mudanças não cancela a distribuição.
2. Abra o *modo de aprovisionamento*.

3 Decida se você deseja distribuir todos os objetos definidos usando o editor da camada de abstração do diretório ou um subconjunto.

- Para distribuir tudo:

  Selecione o nó da raiz, clique o botão direito do mouse e escolha *Distribuir Tudo*

- Para distribuir uma entidade específica, relacionamentos, listas ou definições de configuração:

  Selecione o item em questão, clique o botão direito do mouse e escolha *Distribuir objeto*

Você talvez seja solicitado a informar as credenciais do cofre de identidade. O editor executa uma validação e exibe mensagens de validação em uma caixa de diálogo. Para responder às mensagens de validação, marque ou desmarque os itens a serem distribuídos. Depois de fazer suas seleções de distribuição e submetê-las, você será notificado sobre o sucesso ou a falha da distribuição.

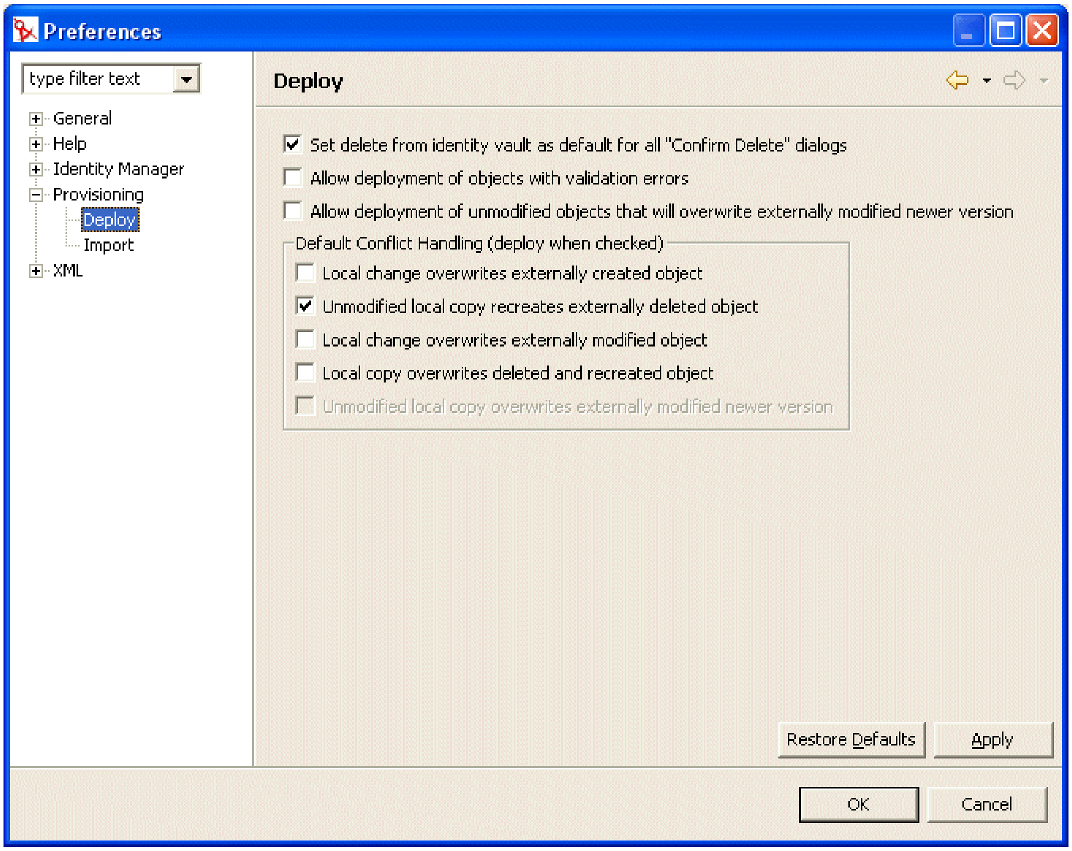
Definindo preferências de distribuição

As preferências de distribuição permitem que você especifique como deseja que o Designer solucione conflitos entre os dados no cofre de identidade e os arquivos da camada de abstração do diretório local. Conflitos podem ocorrer quando outros usuários distribuem mudanças no cofre de identidade, e essas mudanças não são refletidas nas definições do sistema de arquivos local. Para que esses conflitos sejam tratados da forma que você deseja, defina preferências sobre a resolução do conflito.

Para definir preferências de distribuição:

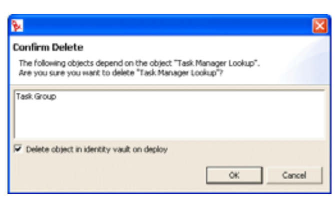
1 Escolha *Janela>Preferências*.

2 Abra o nó de aprovisionamento da árvore e clique em *Distribuir*.



3 Especifique preferências gerais de distribuição:

<table>
<tr><th>Preferência</th><th>Descrição</th></tr>
<tr><td>Defina que a ação padrão de todas as caixas de diálogo “Confirmar Exclusão” seja apagar do cofre de identidade</td><td>Se você tentar apagar um objeto no modo de aprovisionamento ou no editor da camada de abstração do diretório, terá que confirmar a exclusão com uma caixa de diálogo semelhante a esta:



Esta preferência determina se a caixa de confirmação de exclusão **Apagar objeto do cofre de identidade ao distribuir** será selecionada por padrão. Essa preferência indica que a ação padrão é apagar o objeto do cofre de identidade.

O objeto local é sempre apagado.</td></tr>
</table>

Preferência	Descrição
Permitir as distribuições de objetos com erros de validação	**Marcada** — Selecione esta opção se quiser distribuir objetos que não passam na validação. O designer valida as definições que estão sendo distribuídas de acordo com as regras descritas na Seção 4.8, "Importando, validando e distribuindo definições da camada de abstração do diretório" na página 111. **Desmarcada** — Para impedir a distribuição de definições que não passam na validação.
Permitir a distribuição de objetos não modificados que sobregravarão uma versão mais recente modificada externamente	**Marcada** — Se seus arquivos locais não foram mudados, mas os objetos do cofre de identidade foram. Se desejar que os arquivos locais sobregravem os arquivos do cofre de identidade, selecione esta preferência. **Desmarcada** — Se quiser manter as versões mais recentes do cofre de identidade. Quando marcada, você pode definir o comportamento padrão selecionando a preferência de resolução de conflito **Cópia local não modificada sobregrava versão mais recente modificada externamente**.

4 Especifique as preferências de resolução de conflito:

Preferência	Descrição
Mudança local sobregrava objeto criado externamente	**Marcada** — Se você quiser que o objeto que está distribuindo sobregrave o objeto que está no cofre de identidade. **Desmarcada** — A distribuição não ocorre quando há conflito.
Cópia local não modificada recria objeto apagado externamente	**Marcada** — Se você quiser que o objeto local que está distribuindo crie um objeto que já foi apagado do cofre de identidade. **Desmarcada** — A distribuição não ocorre quando há conflito.
Mudança local sobregrava objeto modificado externamente	**Marcada** — Se você quiser que a definição local sempre seja distribuída, mesmo que o cofre de identidade tenha sido mudado por outro usuário. **Desmarcada** — A distribuição não ocorre quando há conflito.
Cópia local sobregrava objeto apagado e recriado	**Marcada** — Se você quiser que o objeto local sempre seja distribuído, mesmo que o objeto do cofre de identidade tenha sido apagado ou apagado e recriado. **Desmarcada** — A distribuição não ocorre quando há conflito.

Preferência	Descrição
Cópia local não modificada sobregrava versão mais recente modificada externamente	Esta preferência só pode ser definida quando a preferência de distribuição geral **Permitir distribuição de objetos não modificados que sobregravará versão mais recente modificada externamente** está selecionada. **Marcada** — Se seus arquivos locais não mudaram, mas os objetos do cofre de identidade mudaram e você **sempre** quer que os arquivos locais sobregravem os arquivos do cofre de identidade como o comportamento padrão. **Desmarcada** — Se quiser manter as versões mais recentes do cofre de identidade.

Configurando o registro

5

Este capítulo inclui o seguinte:

5.1 Sobre o registro de eventos

O aplicativo de usuário do Identity Manager implementa o recurso de registro usando o *log4j*, um pacote de registro de código-fonte aberto distribuído pela Apache Software Foundation. Por padrão, as mensagens de evento são registradas no *console do sistema* e no arquivo de registro do servidor de aplicativos no nível INFO e acima. Você também pode configurar o aplicativo de usuário para registrar no Novell Audit. Os eventos são registrados em *todos* os registradores ativados.

Importante: Se você registra no Novell Audit, é recomendável verificar a documentação do Novell Audit (http://www.novell.com/documentation/nsureaudit).

5.1.1 Sobre as configurações de nível de registro

O registro de console envolve gravações sincronizadas. Isso significa que o registro pode se transformar em um problema de uso do processador, bem como uma impedância de concorrência. Você pode mudar a configuração padrão do valor de prioridade para ERROR, modificando a configuração no <*diretório de instalação*>/jboss/server/IDMProv/conf/log4j.xml. Localize o nó da raiz que se pareça com este:

```
<root> <appender-ref ref="CONSOLE"/> <appender-ref ref="FILE"/> </
root>
```

Mude o valor da prioridade para:

```
<root> <priority value="ERROR"/> <appender-ref ref="FILE"/> </root>
```

Atribuir um valor à raiz garante que qualquer saída (appender) que não tenha um nível explicitamente atribuído herde o nível da raiz. Por padrão a saída file não tem um nível de limite atribuído e portanto, assume o da raiz. Qualquer saída incluída na raiz que tenha um limite deve ser ERROR ou WARN. As configurações de nível de erro que ultrapassam WARN prejudicam o desempenho.

5.2 Registrando em um servidor Novell Audit

Para registrar em um servidor Novell Audit, siga estas etapas:

Etapa	O que fazer	Para obter mais informações
1	Adicionar o esquema do aplicativo Identity Manager ao servidor Novell Audit como um aplicativo de registro	Seção 5.2.1, "Adicionando o esquema do aplicativo Identity Manager ao servidor Novell Audit como um aplicativo de registro" na página 120
2	Configure o **agente de plataforma** do Novell Audit no servidor de aplicativos	O Agente de Plataforma é necessário em todo cliente que reporta eventos ao Novell Audit. Você configura o agente de plataforma com o arquivo de **configuração logevent**. Esse arquivo contém informações de configuração de que o agente de plataforma precisa para se comunicar com o servidor Novell Audit. O local padrão do arquivo no servidor de aplicativos é: ◆ Linux—/etc/logevent.conf ◆ Windows—/<WindowsDir>/logevent.cfg (normalmente c:\windows) Lembre-se de especificar o **endereço IP ou nome DNS do seu servidor Novell Audit** na configuração **LogHost**. Por exemplo: `LogHost=xxx.xxx.xxx.xxx` Especifique outras configurações necessárias ao seu ambiente. **Importante:** Depois de criar ou modificar o arquivo de configuração logevent, é preciso reiniciar o servidor de aplicativos JBoss para que as mudanças sejam ativadas. Para obter mais informações sobre a estrutura do arquivo de configuração logevent, consulte a seção sobre como configurar agentes de plataforma (http://www.novell.com/documentation/nsureaudit) no capítulo sobre o sistema de registro no Guia de Administração do Novell Audit.
3	Habilitar o registro do Novell Audit	Seção 5.2.2, "Habilitando o registro do Audit" na página 121

5.2.1 Adicionando o esquema do aplicativo Identity Manager ao servidor Novell Audit como um aplicativo de registro

Para configurar o Audit para usar o aplicativo de usuário do Identity Manager como um aplicativo de registro, siga estas etapas:

1 Localize o seguinte arquivo:

```
DirXML.lsc
```

Plataforma	Localização
Linux	Após a instalação: `/opt/novell/naudit/logschema/dirxml.lsc`
Windows	Na mídia de instalação: `/nt/dirxml/nsure_audit/nauditextensions/lsc/dirxml.lsc`

2 Use um browser da Web para acessar o *iManager* e efetue login como *administrador*.

3 Vá para *Funções e Tarefas* > *Auditoria e Registro* e selecione *Opções do Servidor de Registro*.

4 Vá até o *container do Serviço de Registro* na sua árvore e selecione o *Servidor de Registro Seguro do Audit* apropriado. Em seguida, clique em *OK*.

5 Vá até a guia *Aplicativos de Registros* , selecione o *Nome do Container* e clique no link *Novo Aplicativo de Registros*.

6 Quando a caixa de diálogo Novo Aplicativo de Registros aparecer, especifique o seguinte:

Para esta configuração	Faça isto
Nome do Aplicativo de Registros	Digite algum nome referente ao seu ambiente
Importar Arquivo LSC	Use o botão **Procurar** para selecionar o arquivo **DirXML.lsc**

Em seguida, clique em *OK*. A guia Aplicativos de Registros exibe o nome de aplicativo adicionado.

7 Clique em *OK* para concluir a configuração do servidor Novell Audit.

8 Verifique se o status do Aplicativo de Registros está definido como ON. (O círculo sob o status deve ser verde. Se estiver vermelho, clique nele para que ele fique ON.)

9 *Reinicie* o servidor Novell Audit para ativar as novas configurações do aplicativo de registros.

5.2.2 Habilitando o registro do Audit

Para habilitar o registro do Novell Audit em seu aplicativo de usuário do Identity Manager

1 Efetue o login no aplicativo de usuário como usuário admin.

2 Selecione a guia *Administração*.

3 Selecione a guia *Registro*.

4 Marque a caixa de seleção *Enviar também mensagens de registro para a Auditoria* (perto da parte inferior da guia).

5 Para manter as mudanças quando o servidor de aplicativos reiniciar outras vezes, a opção *Manter as mudanças no registro* deve estar selecionada.

5.2.3 Os eventos que são registrados

O aplicativo de usuário do Identity Manager registra uma série de eventos automaticamente a partir de solicitações de senha, detalhes, pesquisas e workflow. Por padrão, o aplicativo de usuário do Identity Manager registra automaticamente os seguintes eventos em todos os canais de registro ativos:

ID do evento	Processo	Evento	Gravidade
31400	Portlet Detalhes	Delete_Entity	Informações
31401		Update_Entity	Informações
31410	Portlet Mudar Senha	Change_Password_Failure	Erro
31411		Change_Password_Success	Informações
31420	Portlet Senha Esquecida	Forgot_Password_Change_Failure	Erro
31421		Forgot_Password_Change_Success	Informações
31430	Portlet Pesquisar	Search_Request	Informações
31431		Search_Saved	Informações
31440	Portlet Criar	Create_Entity	Informações

ID do evento	Processo	Evento	Gravidade
31520	Workflow	Workflow_Error	Erro
31521		Workflow_Started	Informações
31522		Workflow_Forwarded	Informações
31523		Workflow_Reassigned	Informações
31524		Workflow_Approved	Informações
31525		Workflow_Refused	Informações
31526		Workflow_Ended	Informações
31527		Workflow_Claimed	Informações
31528		Workflow_Unclaimed	Informações
31529		Workflow_Denied	Informações
3152A		Workflow_Completed	Informações
3152B		Workflow_Timedout	Informações
3152C		User_Message	Informações
31533		Workflow_Retracted	Informações
3152D	Aprovisionamento	Provision_Error	Erro
3152E		Provision_Submitted	Informações
3152F		Provision_Success	Informações
31530		Provision_Failure	Erro
31531		Provision_Granted	Informações
31532		Provision_Revoked	Informações

ID do evento	Processo	Evento	Gravidade
31450	Contexto de Segurança	Create_Proxy_Definition_Success	Informações
31451		Create_Proxy_Definition_Failure	Erro
31452		Update_Proxy_Definition_Success	Informações
31453		Update_Proxy_Definition_Failure	Erro
31454		Delete_Proxy_Definition_Success	Informações
31455		Delete_Proxy_Definition_Failure	Erro
31456		Create_Delegatee_Definition_Success	Informações
31457		Create_Delegatee_Definition_Failure	Erro
31458		Update_Delegatee_Definition_Success	Informações
31459		Update_Delegatee_Definition_Failure	Erro
3145A		Delete_Delegatee_Definition_Success	Informações
3145B		Delete_Delegatee_Definition_Failure	Erro
3145C		Create_Availability_Success	Informações
3145D		Create_Availability_Failure	Erro
3145E		Delete_Availability_Success	Informações
3145F		Delete_Availability_Failure	Erro

5.2.4 Relatórios de registro

Se você registra eventos no canal do banco de dados do Novell Audit, é possível executar relatórios sobre os dados. Existem várias maneiras de gerar relatórios com os dados registrados no banco de dados Novell Audit:

- Use o aplicativo Novell Audit Report para executar seus relatórios ou os relatórios predefinidos descritos em "Relatórios de registro predefinidos" na página 125 a seguir.
- Crie consultas com os dados registrados usando o iManager para selecionar *Auditoria e Registro>Consultas*.
- Crie consultas SQL com os dados registrados.

A tabela padrão do Novell Audit chama-se NAUDITLOG.

Relatórios de registro predefinidos

Os seguintes relatórios de registro predefinidos são criados no formato do Crystal Reports (*.rpt*) para a filtragem de dados registrados no banco de dados Novell Audit:

Nome do relatório	Descrição
Relatório de Ações Administrativas	Mostra todas as ações administrativas iniciadas no portal do aplicativo de usuário do Identity Manager. Este relatório inclui o administrador que iniciou a ação. Ele exclui as mudanças administrativas efetuadas com o iManager ou o Designer for IDM
Relatório do Histórico do Fluxo de Aprovações	Mostra todas as atividades de fluxo de aprovação para um período especificado.
Relatório de Aprovisionamento de Recursos	Mostra todas as atividades de aprovisionamento, classificadas por recurso.
Trilha de Auditoria de Usuário Específico	Mostra toda atividade relacionada a um usuário. As atividades podem ser de aprovisionamento e auto-atendimento.
Relatório de Aprovisionamento de Usuário Específico	Mostra todas as atividades de aprovisionamento para um usuário específico.
Relatório de Aprovisionamento de Usuário	Mostra todas as atividades de aprovisionamento, classificadas por usuário.

Exemplo de relatório Este é um exemplo do relatório Trilha de Auditoria de Usuário Específico:



Novell® Audit Report for Identity Manager

Specific User Audit Trail

Report Period: - 10/13/2005 8:51:32AM

User ID: ablake

Report Last Modified: 10/13/2005
Report Generated On: 10/13/2005
Total pages: 8

Approval Flow

Workflow Event: fecedbe80a3d4abd83c9476a1b576ea2

Date / Time	Action	Initiator ID
9/12/2005 3:20:42PM	Workflow Started	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/12/2005 3:20:43PM	Workflow Forwarded	Workflow Administrator
9/12/2005 3:25:43PM	Workflow Reassigned	Unclaimed
9/12/2005 3:30:44PM	Workflow Forwarded	Workflow Administrator
9/12/2005 3:30:44PM	Workflow Ended	Workflow Administrator
9/12/2005 3:30:44PM	Workflow Denied	System

Workflow Event: fc6d74b1268243b3beac52261439dea0

Date / Time	Action	Initiator ID
9/28/2005 1:12:19PM	Workflow Started	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/28/2005 1:12:22PM	Workflow Forwarded	Workflow Administrator
9/28/2005 2:12:23PM	Workflow Forwarded	Workflow Administrator
9/28/2005 2:12:23PM	Workflow Forwarded	Workflow Administrator
9/28/2005 2:12:23PM	Workflow Forwarded	Workflow Administrator
9/28/2005 2:12:23PM	Workflow Forwarded	Workflow Administrator
9/28/2005 2:12:23PM	Workflow Approved	System
9/28/2005 2:12:23PM	Workflow Approved	System
9/28/2005 2:12:23PM	Workflow Completed	Workflow Administrator
9/28/2005 2:12:27PM	Workflow Forwarded	Workflow Administrator
9/28/2005 2:12:27PM	Workflow Ended	Workflow Administrator
9/28/2005 2:12:27PM	Provision Submitted	Workflow Administrator
9/28/2005 2:12:27PM	Provision Granted	Workflow Administrator

Workflow Event: efaa8304e07641edb9e6375a1a36e396

Date / Time	Action	Initiator ID
10/12/2005 11:58:13AM	Workflow Started	cn=ablake,ou=users,ou=idmsample-qatest,o=novell
10/12/2005 11:58:13AM	Workflow Forwarded	Workflow Administrator

Workflow Event: ea341eb11a824e669e356837745fe264

Date / Time	Action	Initiator ID
9/27/2005 4:24:44PM	Workflow Started	cn=mmackenzie,ou=users,ou=idmsample-Jeff,o=novell
9/27/2005 4:24:44PM	Workflow Forwarded	Workflow Administrator

Page 1 of 8 Specific User Audit Trail

Localização dos arquivos de relatório Os arquivos de relatório estão localizados:

Plataforma	Localização
Windows	/nt/dirxml/reports

Você pode usar esses relatórios como gabaritos para a criação de relatórios personalizados no Crystal Reports Designer. Você também pode executar os relatórios usando o *Relatório de Auditoria* (lreport.exe), um programa do Windows fornecido com o Novell Audit. Os dados de consulta dos relatórios predefinidos do banco de dados de registros padrão do Novell Audit denominado *naudit* e uma tabela de banco de dados chamada *nauditlog*. Se o seu banco de dados de registros do Novell Audit tiver outro nome, use o item de menu *Definir Local da Fonte de Dados* no Crystal Reports Designer para substituir o nome de banco de dados *naudit* por outro de seu ambiente.

Para obter mais informações, consulte a seção sobre como trabalhar com relatórios na documentação do Novell Audit (http://www.novell.com/documentation/nsureaudit).

Administrando o aplicativo de usuário

III

Estes capítulos informam como configurar e gerenciar o aplicativo de usuário do Identity Manager usando a guia Administração da interface de usuário.

Usando a guia Administração

6

Este capítulo apresenta a guia Administração da interface de usuário do Identity Manager. Você aprenderá a usar a guia Administração para configurar e gerenciar o aplicativo de usuário do Identity Manager. Os tópicos incluem:

6.1 Sobre a guia Administração

A interface de usuário do Identity Manager é acessada principalmente pelos usuários finais, que trabalham com as guias nela existentes para aprovisionamento baseado em workflow e auto-atendimento de identidade (com o Módulo de Aprovisionamento do Identity Manager). Porém, essa interface de usuário baseada em browser também tem uma guia chamada *Administração*, que os administradores podem usar para configurar diversas características do *aplicativo de usuário* do Identity Manager subjacente.

Por exemplo, a guia Administração pode ser usada para:

- *Mudar o tema* usado para criar a aparência da interface de usuário
- *Personalizar os recursos de auto-atendimento de identidade* disponíveis para os usuários finais
- *Especificar quem tem permissão* para executar ações administrativas
- *Gerenciar outros detalhes* relativos ao aplicativo de usuário e seu funcionamento

6.2 Quem usa a guia Administração

A guia Administração não está visível aos típicos usuários finais da interface de usuário do Identity Manager. Dois tipos de usuários podem ver e acessar a guia:

- *Administradores de Aplicativo de Usuário*

  Um Administrador de Aplicativo de Usuário tem autorização para realizar todas as funções de gerenciamento relacionadas ao aplicativo de usuário do Identity Manager. Uma dessas funções é acessar a guia Administração da interface de usuário do Identity Manager para executar ações administrativas.

  Durante a instalação, um usuário é especificado como o Administrador de Aplicativo de Usuário. Após a instalação, esse usuário pode utilizar a página *Segurança* da guia Administração para especificar outros Administradores de Aplicativo de Usuário, conforme necessário.

  Para obter detalhes, consulte o Capítulo 11, "Configuração de segurança" na página 207.

- *Usuários permitidos pelos Administradores de Aplicativo de Usuário*

Se necessário, um Administrador de Aplicativo de Usuário pode permitir que um ou mais usuários vejam e acessem páginas específicas da guia Administração. Essas permissões são atribuídas com a página *Admin de Página* da guia Administração.

Para obter detalhes, consulte o Capítulo 7, "Administração de Página" na página 137.

6.3 Acessando a guia Administração

Se você for um Administrador de Aplicativo de Usuário (ou outro usuário permitido), poderá acessar a guia Administração quando precisar gerenciar o aplicativo de usuário do Identity Manager. Você só precisará de um browser da Web suportado.

Para obter uma lista de browsers da Web suportados, consulte o *Novell Identity Manager: Guia de Instalação*.

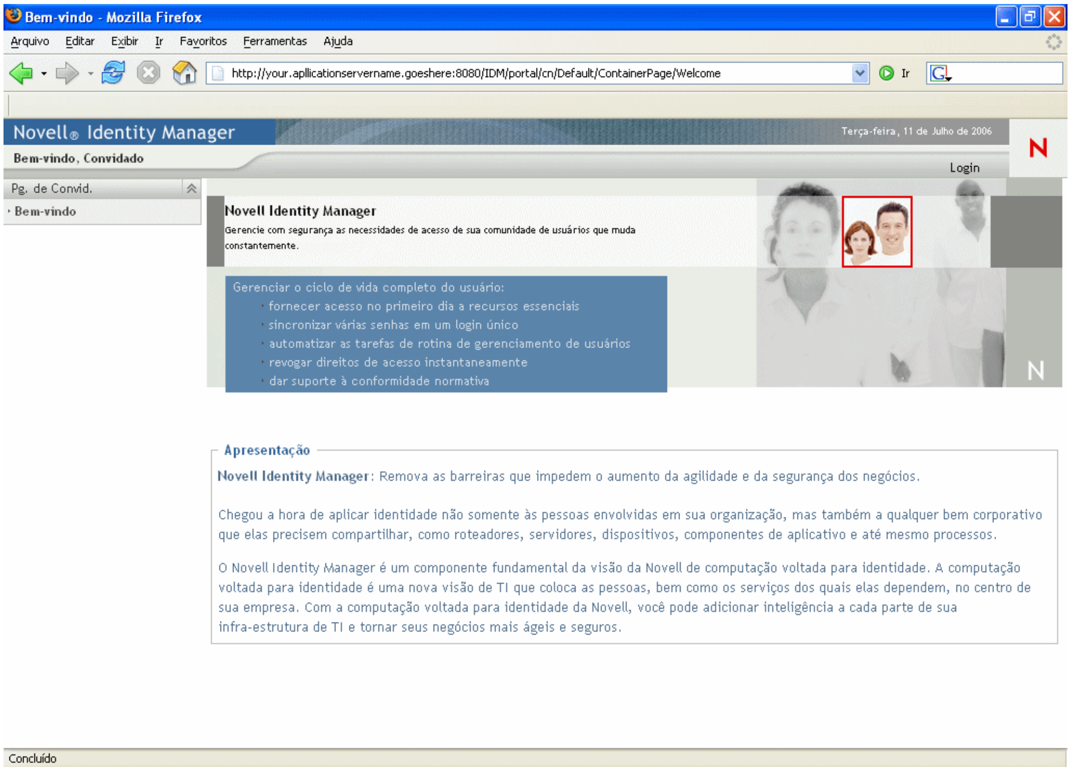
Observação: Para usar a interface de usuário do Identity Manager, verifique se o *JavaScript está habilitado* no browser da Web.

Para acessar a guia Administração:

1 No *browser da Web*, vá até o URL da interface de usuário do Identity Manager (como configurado em seu site). Por exemplo:

```
http://myappserver:8080/IDM
```

A *página de boas-vindas ao convidado* da interface de usuário exibe:



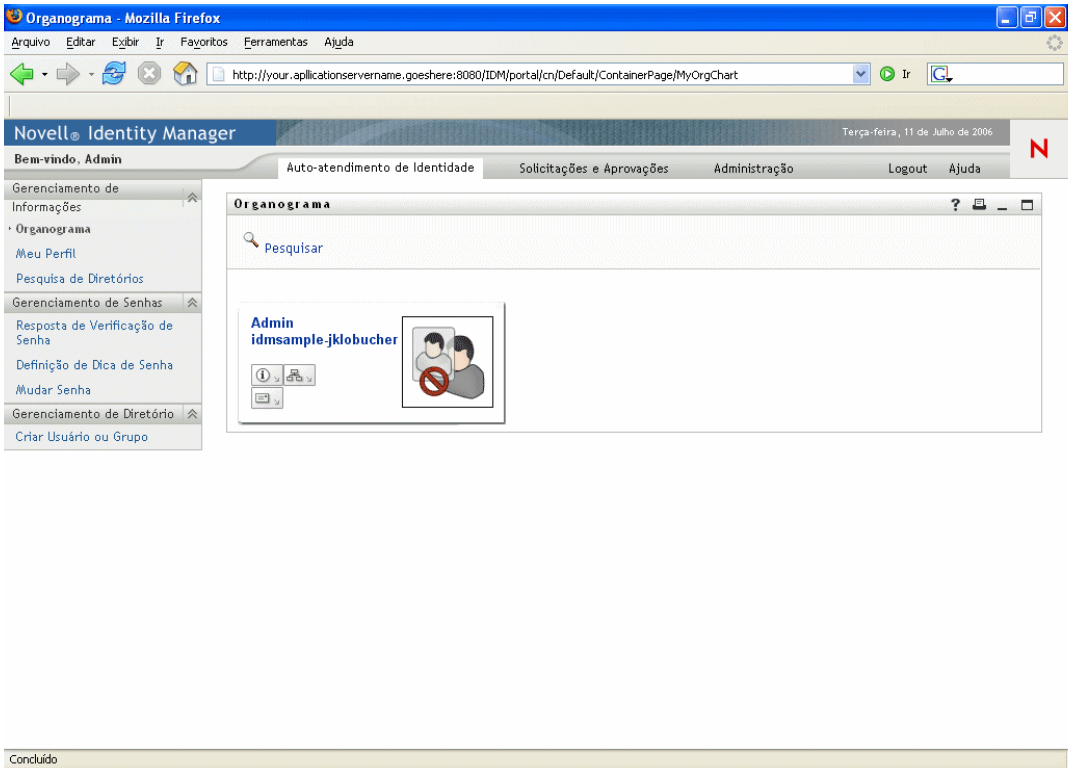
2 Clique no link *Login* no cabeçalho da página.

A interface de usuário solicita seu nome de usuário e sua senha:



3 Informe o nome de usuário e a senha de um *Administrador de Aplicativo de Usuário* (ou um usuário com algumas permissões da guia Administração), e clique em *Login*.

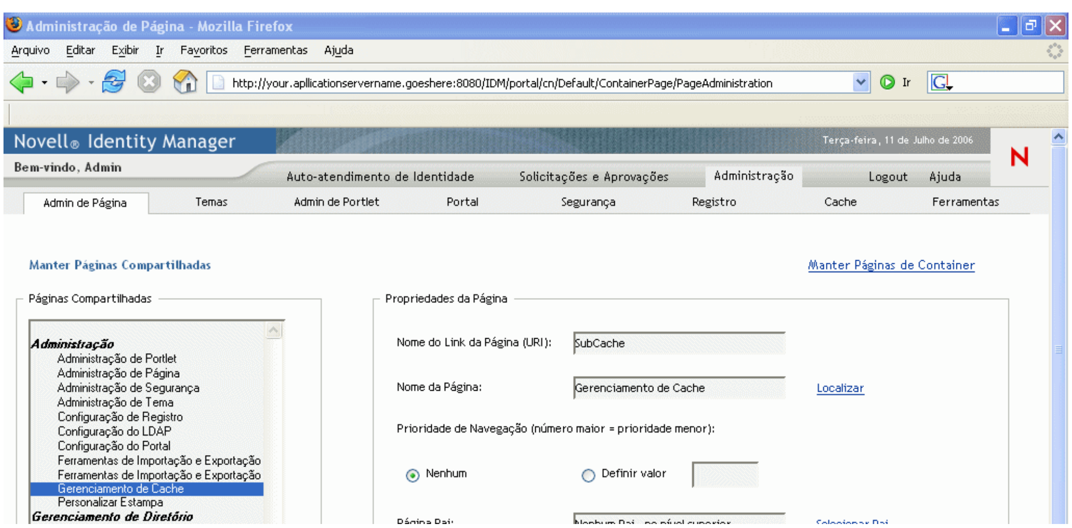
Depois que você se reconectar, verá o conteúdo apropriado da interface desse usuário. Por exemplo:



Por padrão, você está na guia *Auto-atendimento de Identidade*.

4 Clique na guia *Administração*.

A guia Administração exibe um menu das *ações administrativas* que você pode executar. Cada opção tem uma página de configurações e controles correspondente. Por padrão, você vê a página *Admin de Página*:



Para obter informações gerais sobre como acessar e trabalhar na interface de usuário do Identity Manager, consulte o *Aplicativo de Usuário do Identity Manager: Guia do Usuário*.

6.4 Ações administrativas que você pode executar

Na guia Administração, você poderá usar todas as ações disponíveis para configurar e gerenciar o aplicativo de usuário do Identity Manager. Veja este resumo:

Ação	Descrição
Admin de Página	Controla as páginas exibidas na interface de usuário do Identity Manager e quem tem permissão para acessá-las. Para obter detalhes, consulte o Capítulo 7, "Administração de Página" na página 137.
Temas	Controla a aparência da interface de usuário do Identity Manager. Para obter detalhes, consulte o Capítulo 8, "Configuração de tema" na página 173.
Portlet Admin	Controla os portlets exibidos na interface de usuário do Identity Manager e quem tem permissão para acessá-los. Para obter detalhes, consulte o Capítulo 9, "Administração de Portlet" na página 179.
Portal	Controla as características de portal do aplicativo de usuário do Identity Manager e especifica como o usuário se conecta ao cofre de identidade (provedor do LDAP). Para obter detalhes, consulte o Capítulo 10, "Configuração do portal" na página 199.
Segurança	Especifica quem é Administrador de Aplicativo de Usuário no aplicativo de usuário do Identity Manager. Para obter detalhes, consulte o Capítulo 11, "Configuração de segurança" na página 207.
Registro	Controla os níveis de mensagens de registro que o aplicativo de usuário do Identity Manager deve gerar, e especifica se essas mensagens serão enviadas ao Novell Audit. Para obter detalhes, consulte o Capítulo 12, "Configuração de Registro" na página 211.
Cache	Gerencia diversos caches mantidos pelo aplicativo de usuário do Identity Manager. Para obter detalhes, consulte o Capítulo 13, "Configuração de cache" na página 217.
Ferramentas	Permite que você exporte ou importe o conteúdo do portal (páginas e portlets) usado no aplicativo de usuário do Identity Manager. Para obter detalhes, consulte o Capítulo 14, "Ferramentas para a exportação e a importação de dados de portal" na página 227.

Administração de Página

7

Este capítulo informa como usar a página *Administração de Página* da guia *Administração* da interface de usuário do Identity Manager. Os tópicos incluem:

Para obter informações gerais sobre como acessar e trabalhar com a guia Administração, consulte o Capítulo 6, "Usando a guia Administração" na página 131.

7.1 Sobre a administração de página

Você pode usar a página Administração de Página para controlar as *páginas* exibidas na interface de usuário do Identity Manager e quem tem *permissão* para acessá-las. A interface de usuário inclui *dois tipos de páginas*:

Tipo de página	Descrição
Container	As páginas de container conferem às páginas compartilhadas uma aparência consistente, marca corporativa e abordagem de navegação.
Compartilhada	As páginas compartilhadas oferecem um conjunto coerente de conteúdo que é usado para fins específicos (como atualizar o perfil de um usuário). Chamam-se páginas compartilhadas porque oferecem serviços usados por diversas pessoas.

Os dois tipos de página incluem conteúdo na forma de *portlets* (um padrão Java para elementos conectáveis da interface de usuário).

Para saber mais sobre os portlets, consulte o Capítulo 9, "Administração de Portlet" na página 179 e Parte IV, "Referência de portlet" na página 235.

7.1.1 Sobre as páginas de container

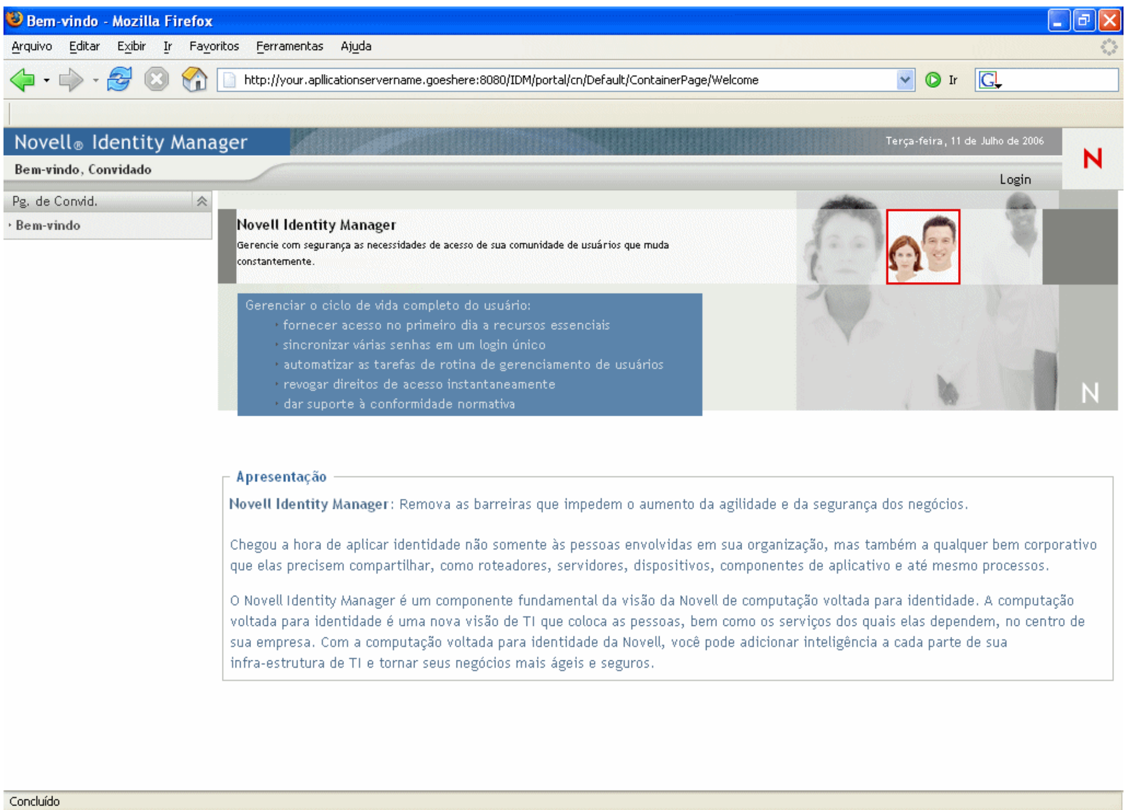
Esta seção apresenta algumas páginas de container que desempenham um papel importante na interface de usuário do Identity Manager.

Lembre-se de que é possível modificar as páginas de container, caso isso seja necessário. Você também pode adicionar suas próprias páginas de container.

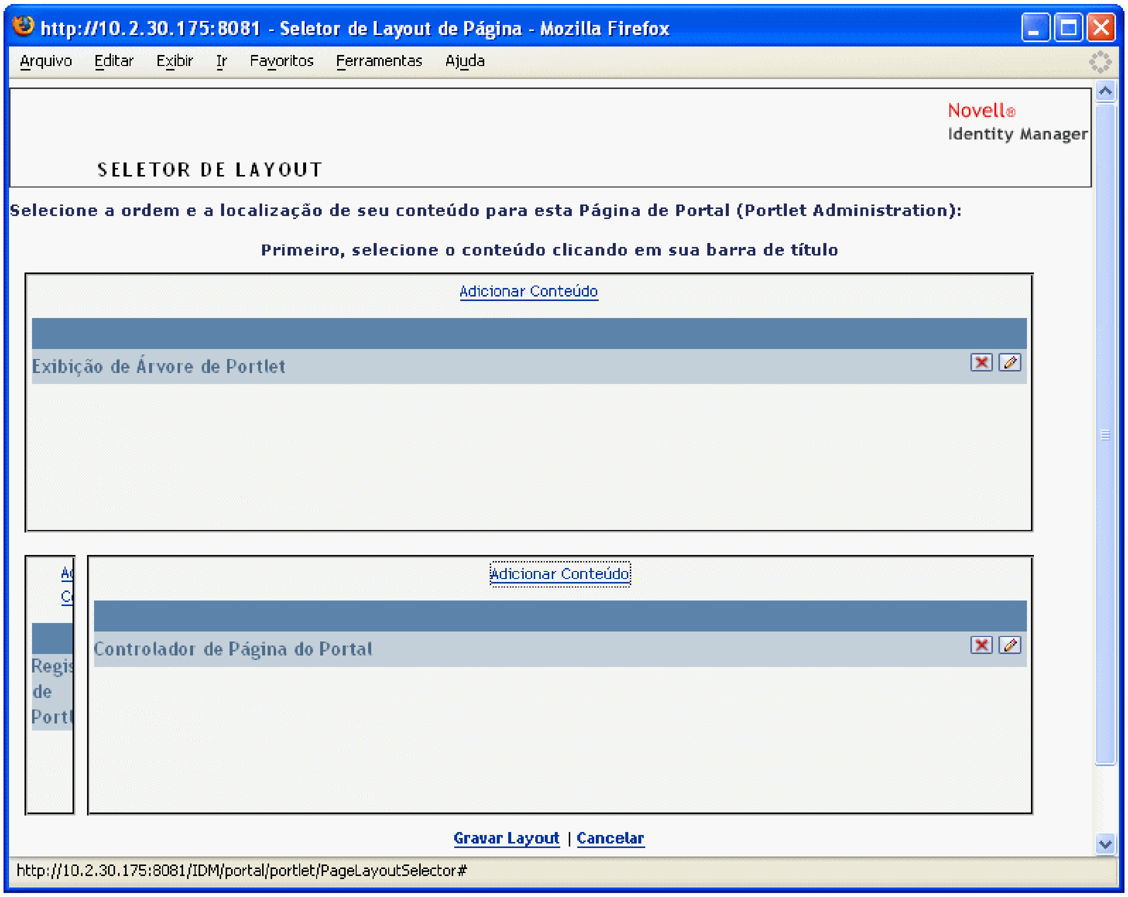
Para saber como trabalhar com as páginas de container, consulte a Seção 7.2, "Criando e mantendo páginas de container" na página 145.

GuestContainerPage

Por padrão, quando os usuários acessam a interface de usuário do Identity Manager, *antes de se conectarem*, eles vêem uma página de container denominada *GuestContainerPage*. Esta é a página de container:



Internamente, GuestContainerPage tem o seguinte *layout*:



O layout de GuestContainerPage divide-se em *três regiões*, que exibem os seguintes portlets:

Portlet	Descrição
HeaderPortlet	Exibe as informações de cabeçalho e os controles da guia de nível superior da interface de usuário
Navegação de Página Compartilhada	Exibe um menu vertical onde o usuário pode selecionar uma página compartilhada para exibição
Controlador de Página do Portal	Exibe a página compartilhada que o usuário selecionou no momento pelo portlet Navegação de Página Compartilhada.

Por padrão, somente os seguintes itens desses portlets podem ser visualizados pelos usuários antes de se conectarem:

- Um único link no cabeçalho: *Login*
- Uma única página compartilhada *Bem-vindo*

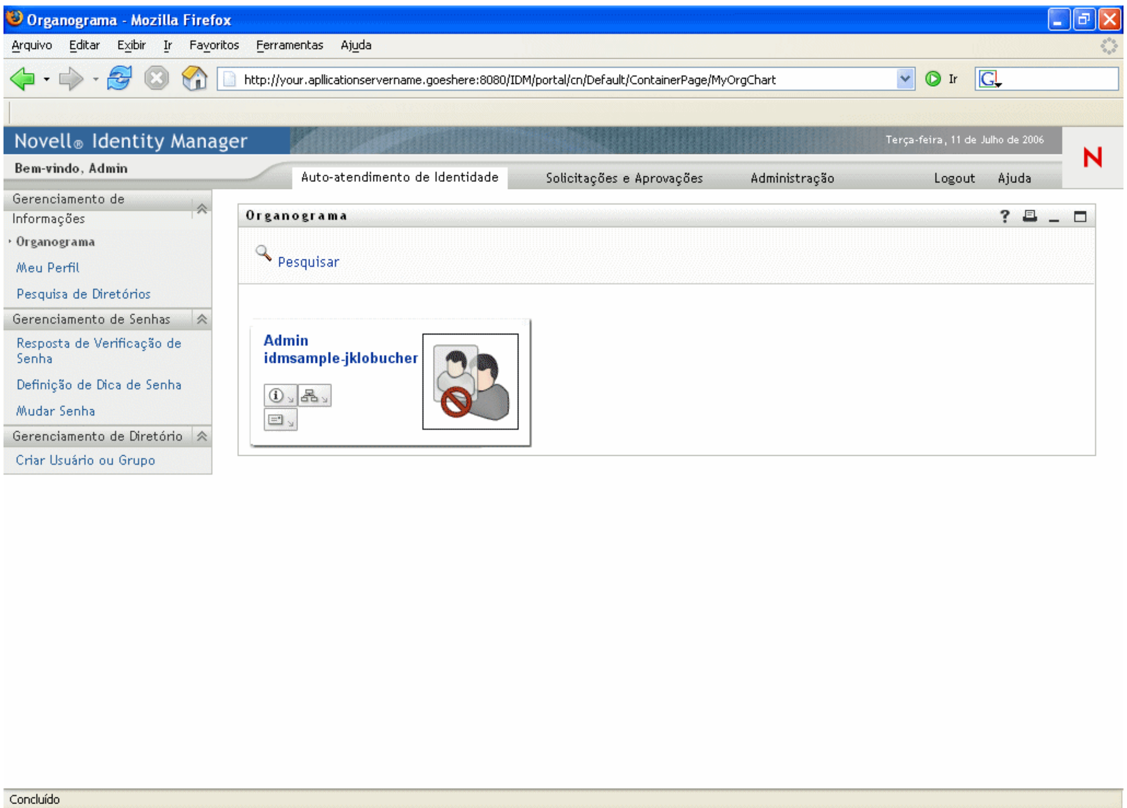
Como o usuário ainda não está conectado, o portlet Navegação de Página Compartilhada mostra apenas as páginas compartilhadas que estão na categoria *Páginas de Convidados*; e não exibe nenhuma das outras categorias. Por padrão, a página Bem-vindo é a única na categoria Páginas de Convidados.

Após o login, o portlet Navegação de Página Compartilhada não exibe a categoria Páginas de Convidados. Ele passa a mostrar outras categorias de páginas compartilhadas (como especificado nas preferências).

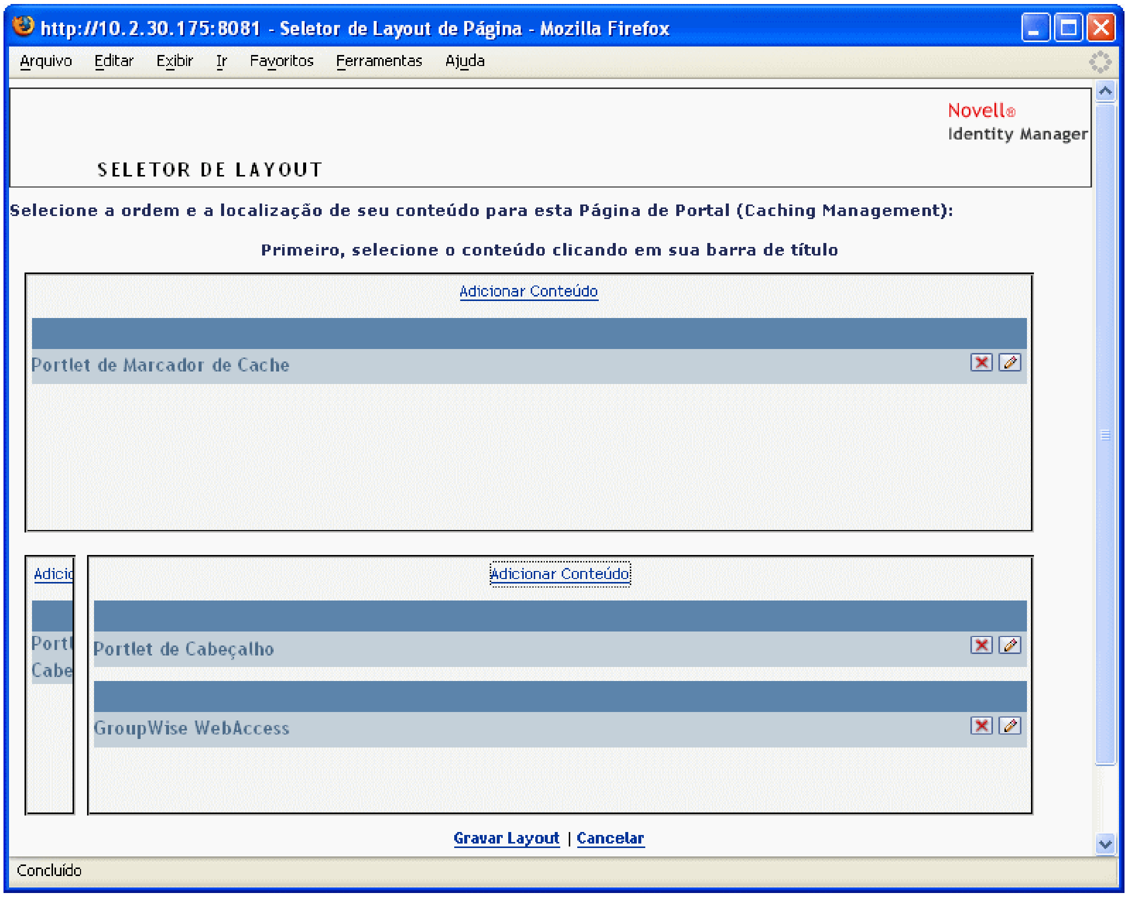
Para obter mais informações sobre o portlet Navegação de Página Compartilhada, consulte o Capítulo 15, "Sobre os portlets" na página 237.

DefaultContainerPage

Por padrão, *depois de efetuar login* na interface de usuário do Identity Manager, os usuários vão para a página de container chamada *DefaultContainerPage*. Esta é a página de container:



Internamente, DefaultContainerPage tem o seguinte *layout*:



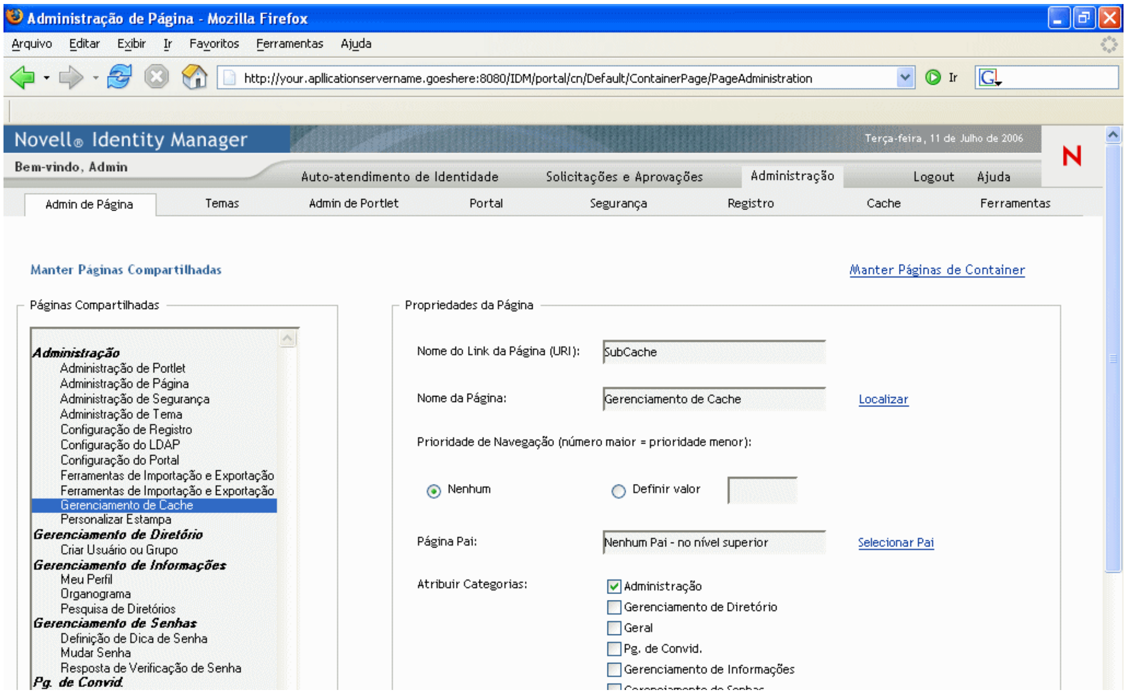
O layout de DefaultContainerPage divide-se em *três regiões*, que exibem os seguintes portlets:

Portlet	Descrição
HeaderPortlet	Exibe as informações de cabeçalho e os controles da guia de nível superior da interface de usuário
Navegação de Página Compartilhada	Exibe um menu vertical onde o usuário pode selecionar uma página compartilhada para exibição
Controlador de Página do Portal	Exibe a página compartilhada que o usuário selecionou no momento pelo portlet Navegação de Página Compartilhada.
Aviso de Tempo de Espera da Sessão	Exibe uma mensagem de alerta sempre que uma sessão de usuário está para entrar em tempo de espera

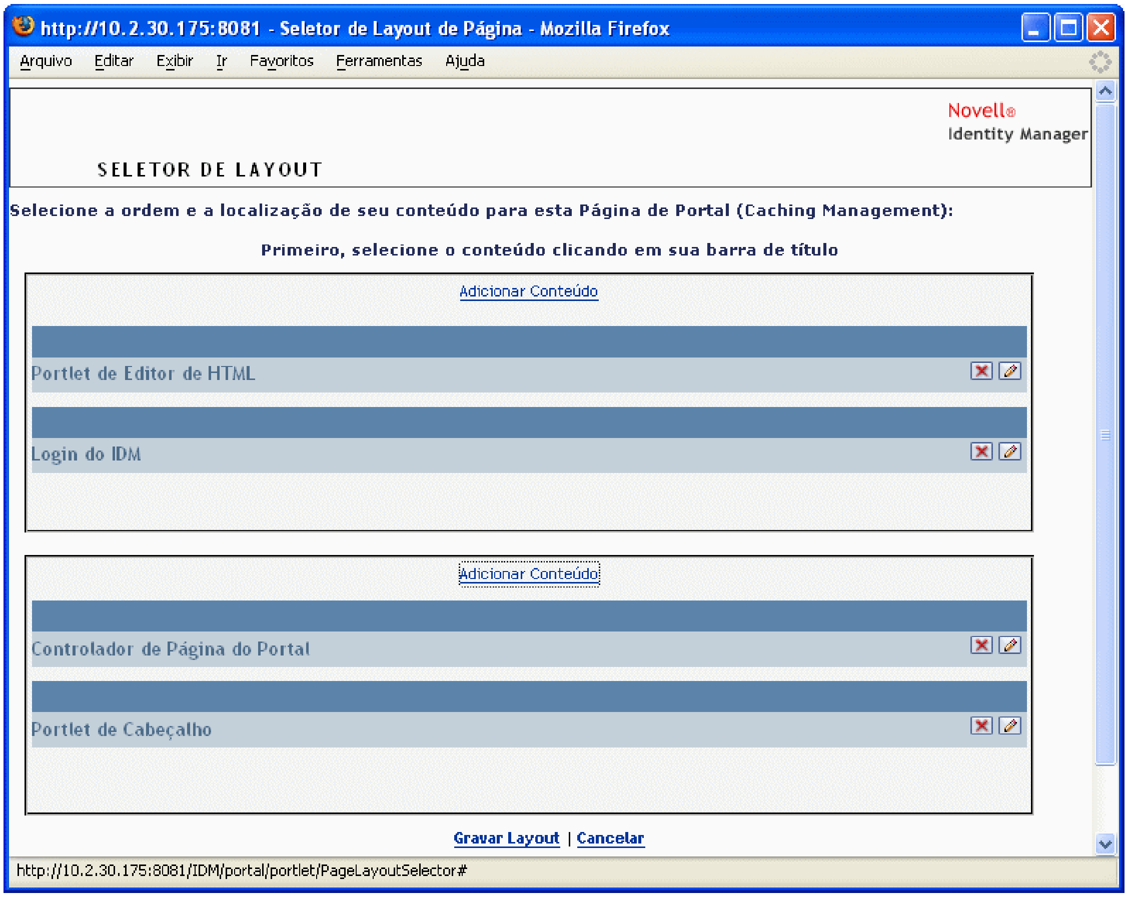
Lembre-se de que depois que o usuário efetuar login, *DefaultContainerPage abrirá automaticamente a guia Auto-atendimento de Identidade* no HeaderPortlet.

Página de Container de Admin

Por padrão, quando Administradores de Aplicativo de Usuário (e outros usuários autorizados) *clicam na guia Administração* da interface de usuário do Identity Manager, eles acessam uma página de container denominada *Página de Container de Admin*. Esta é a página de container:



Internamente, a Página de Container de Admin tem o seguinte *layout*:



O layout da Página de Container de Admin divide-se em *duas regiões*, que exibem os seguintes portlets:

Portlet	Descrição
HeaderPortlet	Exibe as informações de cabeçalho e os controles da guia de nível superior da interface de usuário
Exibição da Lista de Admin	Exibe um segundo nível de guias onde o usuário pode selecionar uma ação administrativa para execução
Controlador de Página do Portal	Exibe uma página compartilhada que corresponde à guia que o usuário selecionou no momento pelo portlet Exibição da Lista de Admin.
Aviso de Tempo de Espera da Sessão	Exibe uma mensagem de alerta sempre que uma sessão de usuário está para entrar em tempo de espera

7.1.2 Sobre as páginas compartilhadas

A identidade de usuário do Identity Manager inclui muitas páginas compartilhadas que fornecem o principal conteúdo em suas páginas de container. É possível modificar as páginas compartilhadas, caso isso seja necessário. Você também pode adicionar suas próprias páginas compartilhadas.

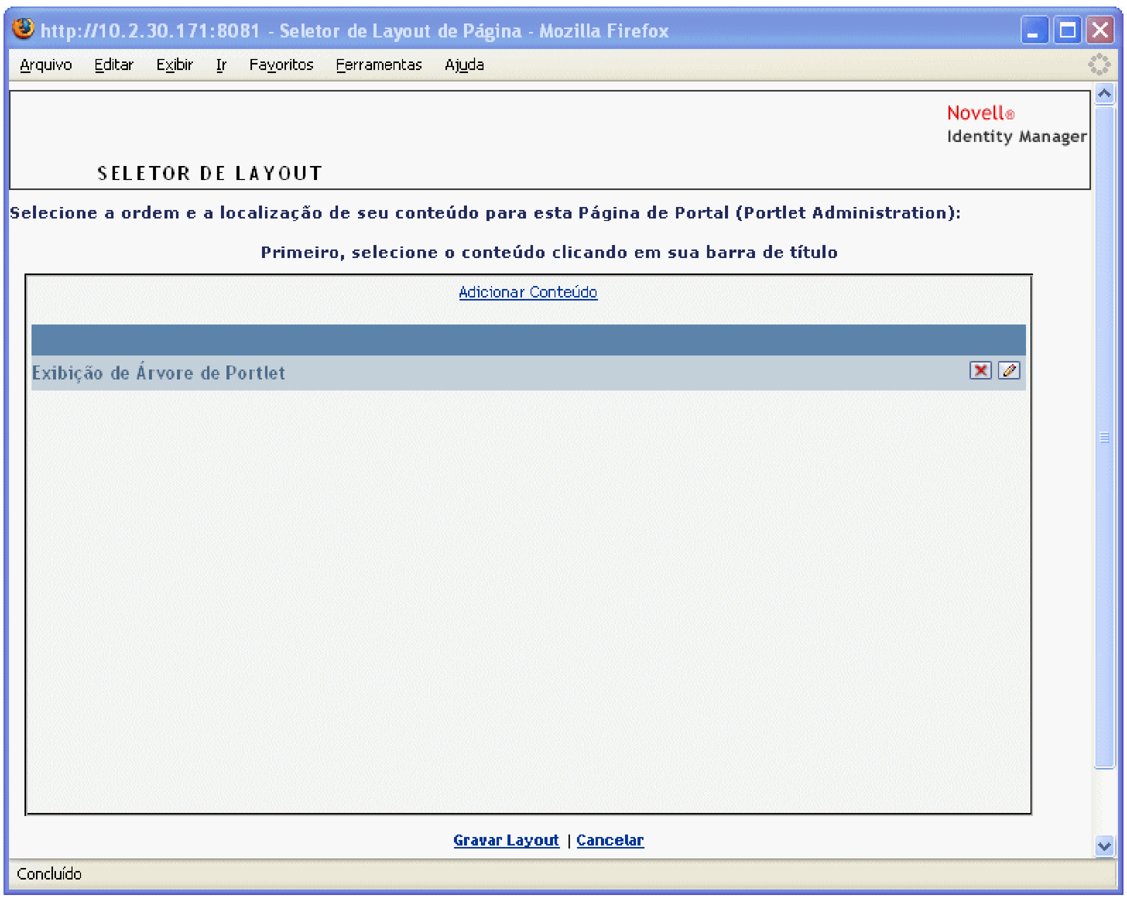
Para saber como trabalhar com as páginas compartilhadas, consulte a Seção 7.3, “Criando e mantendo páginas compartilhadas” na página 154.

Uma típica página compartilhada

Vamos verificar uma dessas páginas compartilhadas. *Organograma* é a *página compartilhada padrão* que DefaultContainerPage exibe depois que os usuários efetuam login na interface de usuário do Identity Manager:



Internamente, Organograma tem o seguinte *layout*:



O layout de Organograma consiste em apenas *uma região*, que exibe somente um portlet (o portlet *Organograma*).

7.1.3 Uma exceção para o uso da página

Neste capítulo você verificou como essas guias de nível superior da interface de usuário do Identity Manager baseiam-se em páginas:

- A *guia Auto-atendimento de Identidade* usa a *DefaultContainerPage*
- A *guia Administração* usa a *Página de Container de Admin*

Contudo, lembre-se de que a *guia Solicitações e Aprovações* baseia-se em uma arquitetura diferente e *não pode ser manipulada* pela Administração de Página.

7.2 Criando e mantendo páginas de container

O processo de criar e manter páginas de container envolve as seguintes etapas:

1. *Crie* uma nova página de container ou *selecione* uma página de container existente, como descrito na Seção 7.2.1, "Criando páginas de container" na página 145.
2. *Adicione conteúdo* (na forma de portlets) à página, como descrito na Seção 7.2.2, "Adicionando conteúdo a uma página de container" na página 148.

   Você também pode *apagar conteúdo* da página, como descrito na Seção 7.2.3, "Apagando conteúdo de uma página de container" na página 149.
3. *Escolha um layout de portal*, como descrito na Seção 7.2.4, "Modificando o layout de uma página de container" na página 150.
4. *Ordene e posicione* conteúdo no layout selecionado, como descrito na Seção 7.2.5, "Organizando conteúdo na página de container" na página 151.
5. *Exiba a nova página* inserindo o URL da página de container no seu browser, como descrito na Seção 7.2.6, "Exibindo uma página de container" na página 153.

Páginas de container e layouts As páginas de container estão estreitamente vinculadas a layouts de portal. Isso significa que você pode alternar layouts de páginas de container sem perder seu conteúdo. Quando você aplica um novo layout a uma página de container, os portlets que foram adicionados à página são exibidos automaticamente com o novo layout. Pode ser necessário ajustar o posicionamento do conteúdo no novo layout.

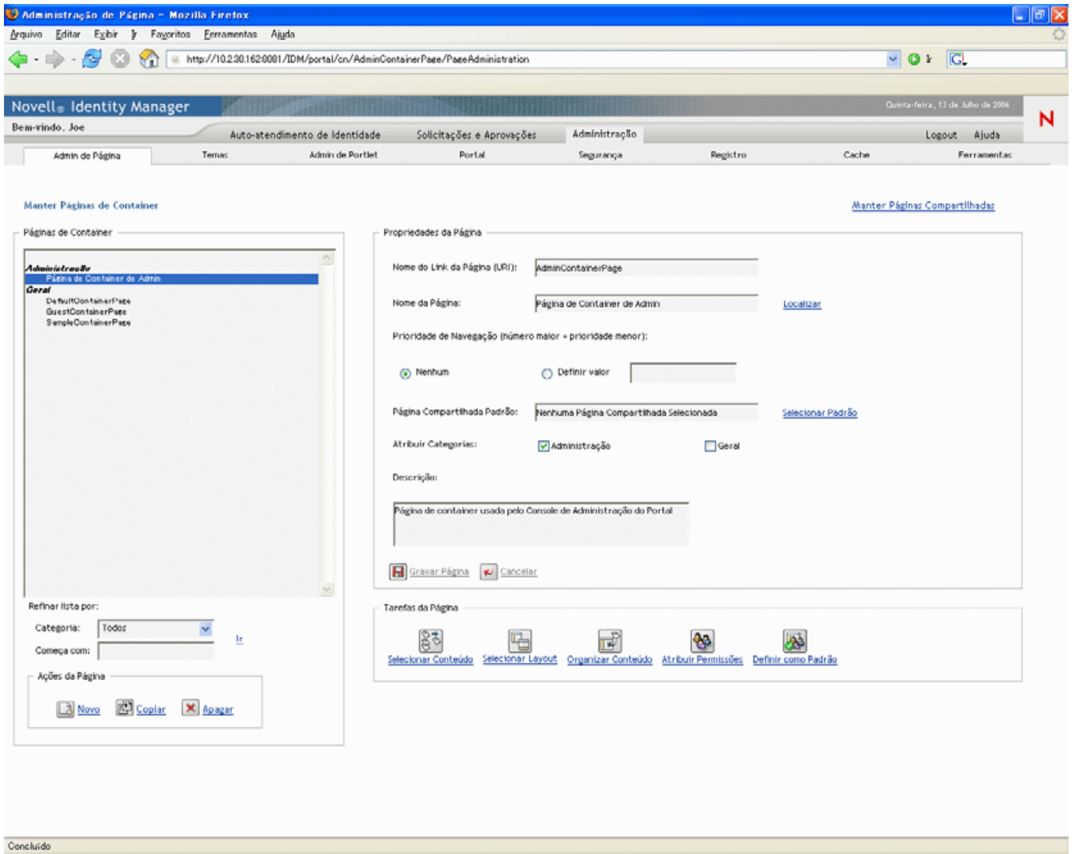
7.2.1 Criando páginas de container

Você pode criar páginas de container do zero ou copiar páginas já existentes. Esta seção descreve os dois procedimentos.

Para criar uma página de container do zero:

1. Na página Administração de Página, selecione *Manter Páginas de Container*.

O painel Manter Páginas de Container é exibido:



2 Selecione a ação da página *Novo* (na seção inferior esquerda do painel).

Uma página sem título nem categoria é criada.

3 Especifique as *propriedades* da página de container:

Propriedade	O que fazer

Nome do Link da Página (URI)	Especifique o nome de URI da página (como ele deve aparecer no URL da interface de usuário). Por exemplo, se você especificar o URI:
	
	`MyContainerPage`
	
	ele aparecerá no URL da seguinte maneira:
	
	`http://myappserver:8080/IDM/portal/cn/`
	`MyContainerPage`

Propriedade	O que fazer
Nome da Página	Especifique o nome de exibição da página. Por exemplo: `My Container Page` Você pode clicar em **Localizar** para especificar versões localizadas deste nome para outros idiomas.
Prioridade de Navegação	Especifique uma das seguintes opções: ◆ **Nenhum** — se não houver necessidade de atribuir uma prioridade à página de container. ◆ **Definir valor** — para atribuir uma prioridade a uma página de container em relação a outras páginas de container. A prioridade deve ser um número inteiro entre -1 e 9999, onde -1 é a prioridade mais alta e 9999 é a mais baixa. A definição de valores de prioridade é útil quando você quer garantir uma ordem específica para a listagem das páginas por prioridade, ou se você desejar garantir determinada seleção quando houver várias páginas padrão (no caso de usuário que pertence a diversos grupos).
Página Compartilhada Padrão	Consulte a Seção 7.6, "Selecionando uma página de container padrão para uma página de container" na página 171.
Atribuir Categorias	Selecione zero ou mais das seguintes categorias a que a página deve pertencer: ◆ Administração ◆ Geral A atribuição de categorias é útil quando você deseja assegurar a organização da listagem das páginas por categoria, ou se você pretende garantir um subconjunto apropriado quando as páginas são filtradas por categoria.
Descrição	Digite um texto que descreva a página.

4 Clique em *Gravar Página* (na parte inferior da seção de propriedades da página).

Para criar uma página de container copiando uma página já existente:

1 Na página Administração de Página, selecione *Manter Páginas de Container*.

O painel Manter Páginas de Container é exibido (como indicado no procedimento anterior).

2 Na lista de páginas de container, *selecione* a página a ser copiada.

Dica: Se a lista for longa, você pode *refiná-la* (por categoria ou texto inicial) para encontrar a página desejada mais facilmente.

3 Selecione a ação da página *Copiar* (na seção inferior esquerda do painel).

Uma nova página de container será criada com o nome *Cópia de NomeDePáginaOriginal*.

4 Especifique as *propriedades* da página de container (como descrito no procedimento anterior).

5 Clique em *Gravar Página* (na parte inferior da seção de propriedades da página).

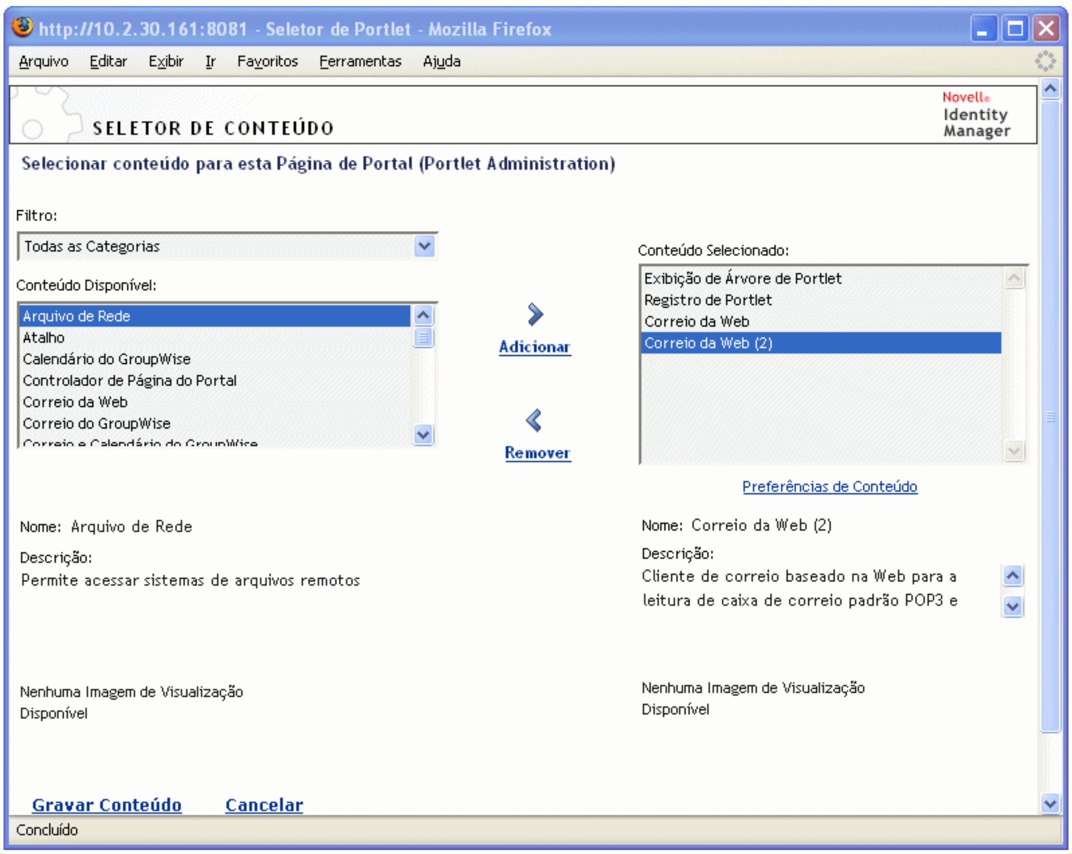
7.2.2 Adicionando conteúdo a uma página de container

Depois de criar uma página de container, a próxima etapa é adicionar conteúdo. Para isso, selecione os portlets a serem inseridos na página. Você pode usar portlets pré-elaborados que são fornecidos com o aplicativo de usuário do Identity Manager ou outros portlets que você tenha registrado.

Para adicionar conteúdo a uma página de container:

1 Abra uma página nova ou existente no painel Manter Páginas de Container e clique na tarefa da página *Selecionar Conteúdo* (na parte inferior do painel).

O *Seletor de Conteúdo* é exibido em uma nova janela do browser:



2 Se você quiser exibir uma categoria específica de conteúdo disponível, selecione uma categoria no menu suspenso *Filtrar*.

3 Selecione um ou mais portlets na lista de *Conteúdo Disponível*.

Dica: Mantenha a tecla *Control* pressionada para selecionar vários portlets não contíguos na lista. Use a tecla *Shift* para fazer várias seleções contíguas.

---

4 Clique em *Adicionar* para transferir suas escolhas para a lista de *Conteúdo Selecionado*.

5 Você pode clicar em *Preferências de Conteúdo* para editar as preferências de qualquer portlet que tenha selecionado para a página de container. Os valores de preferência especificados são ativados na instância do portlet exibida em sua página.

6 Clique em *Gravar Conteúdo*.

Depois de escolher o conteúdo da página de container, você pode selecionar um novo layout, como descrito na Seção 7.2.4, "Modificando o layout de uma página de container" na página 150, ou organizar o conteúdo no layout atual, como descrito na Seção 7.2.5, "Organizando conteúdo na página de container" na página 151.

7.2.3 Apagando conteúdo de uma página de container

No processo de criar páginas de container, para apagar conteúdo, você deve remover os portlets da página. Você pode usar o Seletor de Conteúdo ou o Seletor de Layout, como descrito nos procedimentos a seguir.

Para apagar conteúdo de uma página de container usando o Seletor de Conteúdo:

1. Abra uma página no painel Manter Páginas de Container e clique na tarefa da página *Selecionar Conteúdo* (na parte inferior do painel).

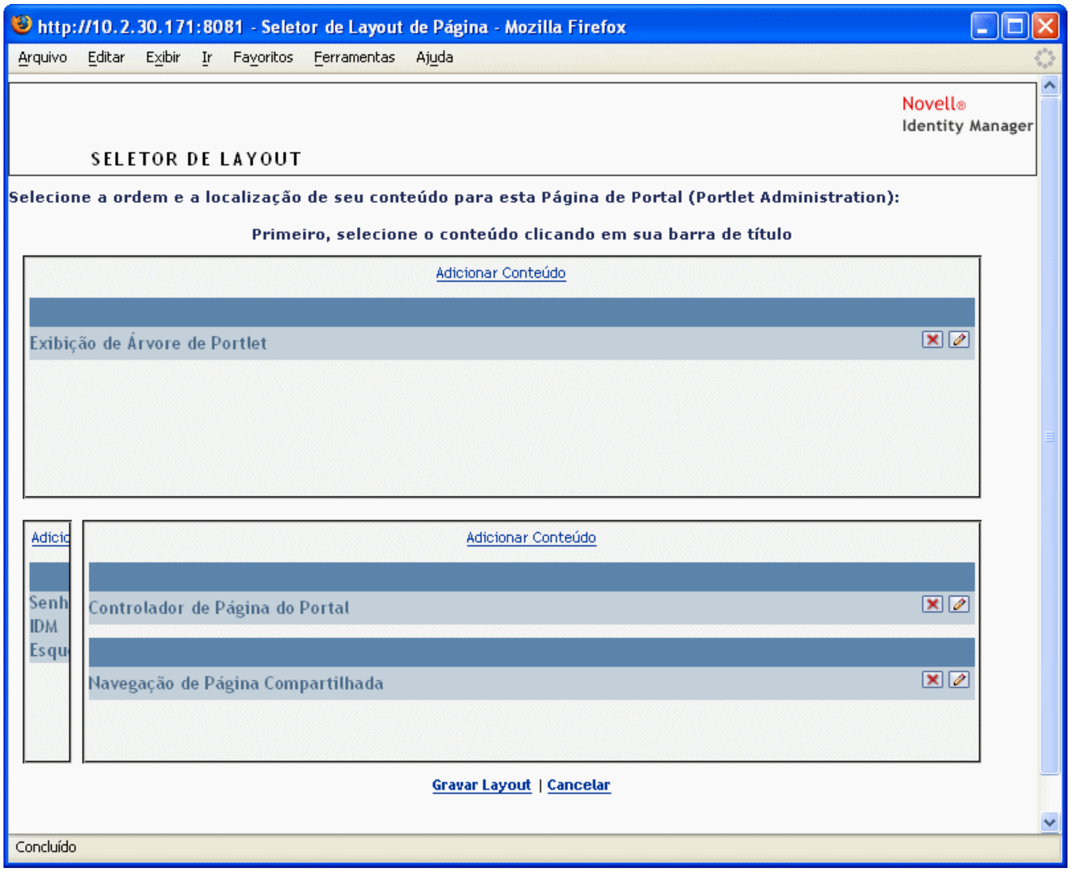
   O *Seletor de Conteúdo* é exibido em uma nova janela do browser (como indicado no procedimento anterior).
2. Na lista Conteúdo Selecionado, escolha um portlet para ser apagado e clique em *Remover*.

   O portlet é removido da página.
3. Clique em *Gravar Conteúdo*.

Para apagar conteúdo de uma página de container usando o Seletor de Layout:

1. Abra uma página no painel Manter Páginas de Container e clique na tarefa da página *Organizar Conteúdo* (na parte inferior do painel).

O *Seletor de Layout* é exibido em uma nova janela do browser, mostrando os portlets dessa página:



2 Clique no botão *X* de um portlet a ser removido.

3 Ao ser solicitado, clique em *OK* para confirmar.

O portlet é removido da página.

4 Clique em *Gravar Layout*.

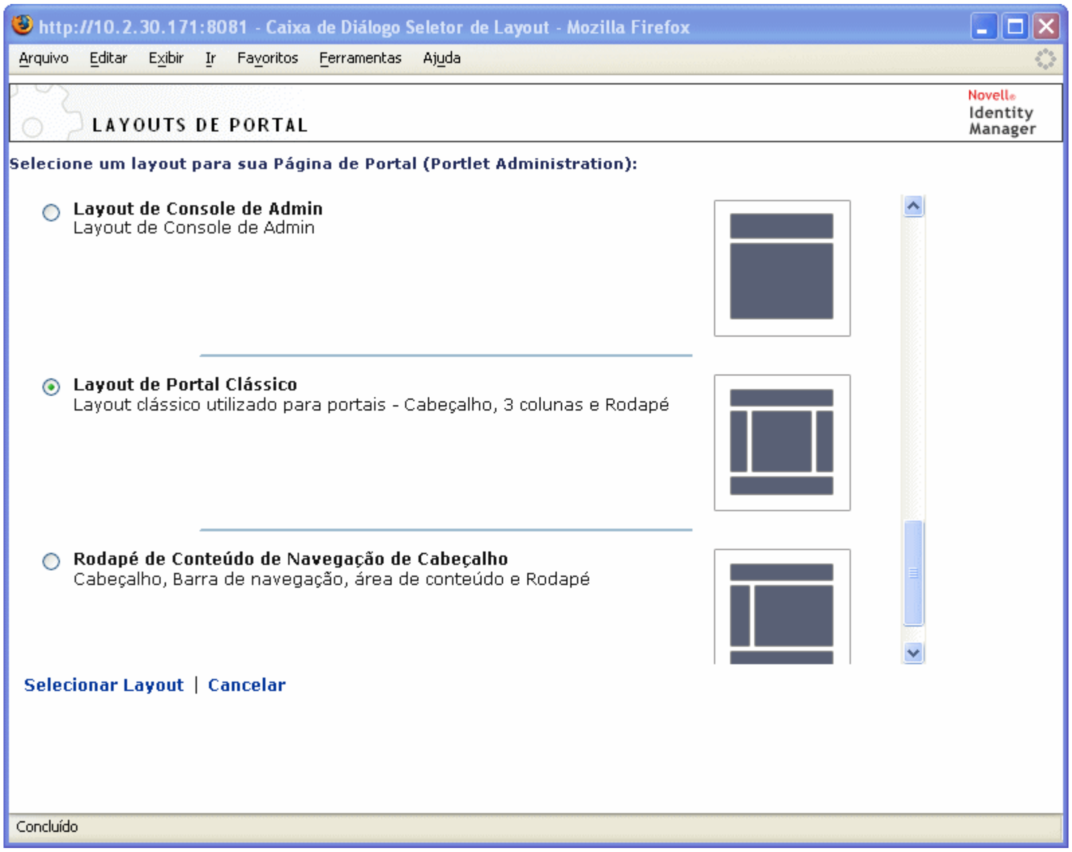
7.2.4 Modificando o layout de uma página de container

Quando você modifica o layout de uma página de container, o conteúdo existente é reorganizado para acomodar-se ao novo layout. Em alguns casos, pode ser necessário ajustar o resultado final.

Para modificar o layout de uma página de container:

1 Abra uma página no painel Manter Páginas de Container e clique na tarefa da página *Selecionar Layout* (na parte inferior do painel).

A lista *Layouts de Portal* é exibida em uma nova janela do browser:



2 *Percorra* as opções e *selecione* o layout desejado.

3 Clique em *Selecionar Layout*.

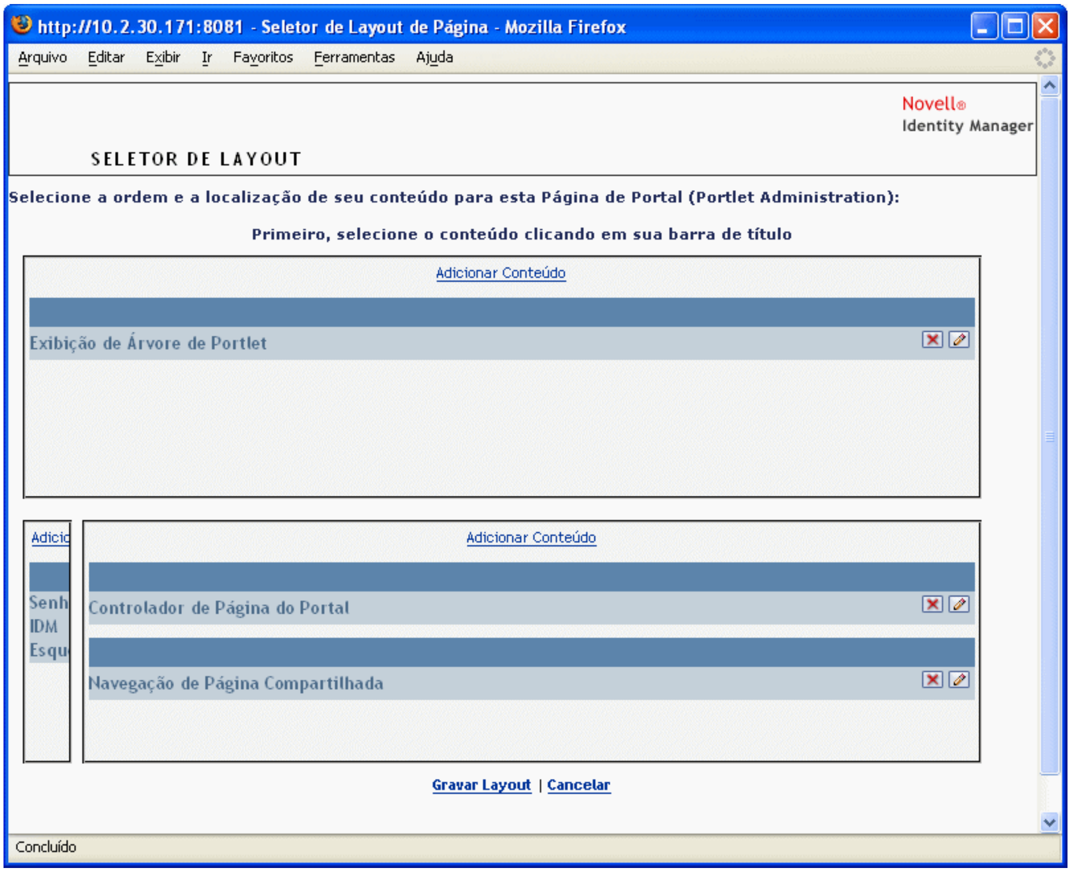
7.2.5 Organizando conteúdo na página de container

Depois de designar o conteúdo e o layout da página de container, você pode posicionar o conteúdo no layout, adicionar outros portlets em locais específicos ou apagar portlets.

Para organizar conteúdo em uma página de container:

1 Abra uma página no painel Manter Páginas de Container e clique na tarefa da página *Organizar Conteúdo* (na parte inferior do painel).

O *Seletor de Layout* é exibido em uma nova janela do browser, mostrando os portlets dessa página:



2 Se quiser *adicionar um portlet* à página, siga estas etapas:

2a Clique em *Adicionar Conteúdo* no frame de layout desejado.

O *Seletor de Portlet* é exibido em uma nova janela do browser.

2b Se você quiser exibir uma categoria específica de conteúdo disponível, selecione uma categoria no menu suspenso *Filtrar*.

2c Selecione um portlet na lista de *Conteúdo Disponível*.

2d Clique em *Selecionar Conteúdo*.

O Seletor de Portlet fecha e o portlet selecionado aparece no frame de layout de destino do Seletor de Layout.

3 Se você quiser *mover um portlet* para outra parte do layout, siga estas etapas específicas ao browser:

Browser	O que fazer
Internet Explorer	1. Mova o cursor sobre a barra de título do portlet até ele assumir a forma de uma mão. 2. Mantenha o botão esquerdo do mouse pressionado e arraste o portlet até o local desejado no layout.
Mozilla	1. Clique no portlet que deseja mover. 2. Clique dentro do frame de layout de destino.
	O portlet é transferido.

4 Se quiser *remover um portlet* do layout, siga estas etapas:

4a Clique no botão *X* do portlet a ser removido.

4b Ao ser solicitado, clique em *OK* para confirmar.

O portlet é removido do layout.

5 Se quiser *editar as preferências* de um portlet, siga estas etapas:

5a Clique no botão de *lápis* do portlet a ser editado.

As *Preferências de Conteúdo* do portlet são exibidas no browser.

5b *Mude* os valores da preferência conforme apropriado.

Os valores de preferência especificados são ativados na instância do portlet exibida em sua página.

5c Clique em *Gravar Preferências*.

6 Clique em *Gravar Layout* para registrar as mudanças e fechar o Seletor de Layout.

7.2.6 Exibindo uma página de container

Para exibir sua página, vá até o URL da página de container no seu browser.

Para exibir uma página de container

- No seu *browser da Web*, vá até o seguinte URL:

```
http://server:port/IDM-war-context/portal/cn/container-page-name
```

Por exemplo, para exibir a página de container *MyContainerPage*:

```
http://myappserver:8080/IDM/portal/cn/MyContainerPage
```

7.3 Criando e mantendo páginas compartilhadas

O processo de criar e manter páginas compartilhadas envolve as seguintes etapas:

1. *Crie* uma nova página compartilhada ou *selecione* uma página compartilhada existente, como descrito na Seção 7.3.1, “Criando páginas compartilhadas” na página 154.
2. *Adicione conteúdo* (na forma de portlets) à página, como descrito na Seção 7.3.2, “Adicionando conteúdo a uma página compartilhada” na página 157.

   Você também pode *apagar conteúdo* da página, como descrito na Seção 7.3.3, “Apagando conteúdo de uma página compartilhada” na página 159.
3. *Escolha um layout de portal*, como descrito na Seção 7.3.4, “Modificando o layout de uma página compartilhada” na página 160.
4. *Ordene e posicione* conteúdo no layout selecionado, como descrito na Seção 7.3.5, “Organizando conteúdo na página compartilhada” na página 161.
5. *Exiba a nova página* inserindo o URL da página compartilhada no seu browser, como descrito na Seção 7.2.6, “Exibindo uma página de container” na página 153.

Páginas compartilhadas e layouts As páginas compartilhadas estão estreitamente vinculadas a layouts de portal. Isso significa que você pode alternar layouts de páginas compartilhadas sem perder seu conteúdo. Quando um novo layout é aplicado, os portlets que foram adicionados à página são exibidos automaticamente com o novo layout. Pode ser necessário ajustar o posicionamento do conteúdo no novo layout.

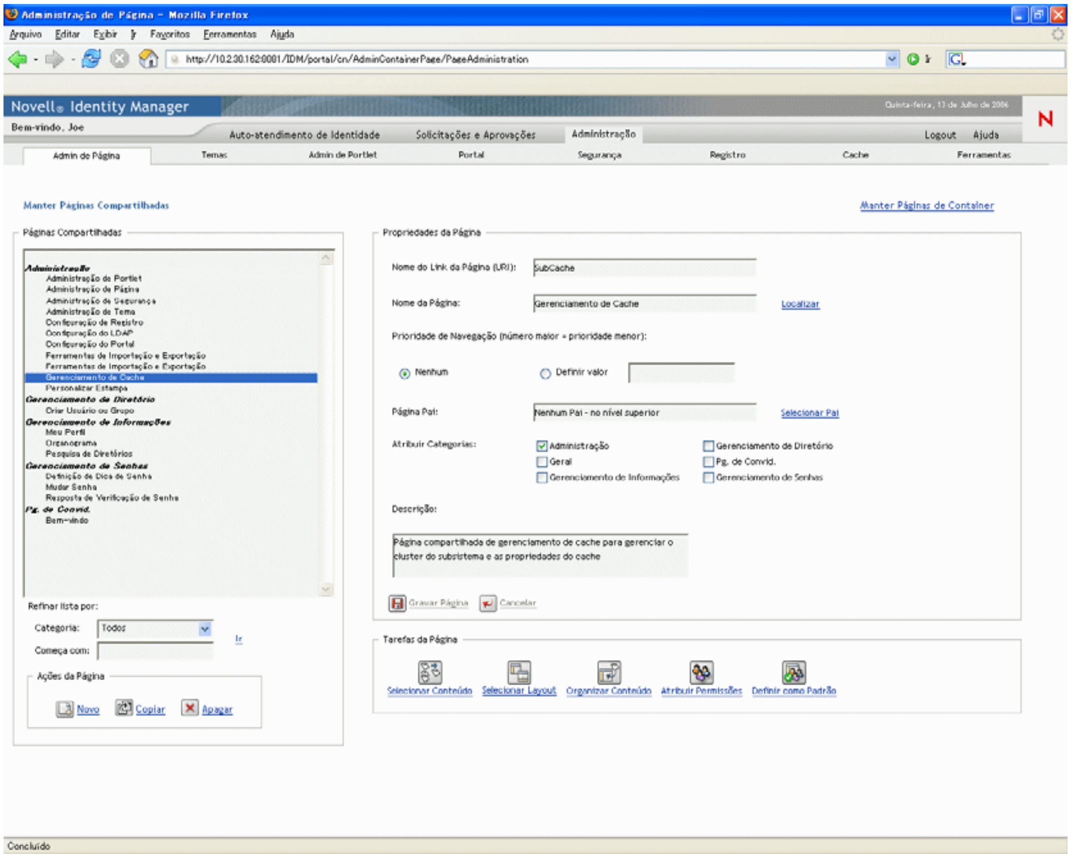
7.3.1 Criando páginas compartilhadas

Você pode criar páginas compartilhadas do zero ou copiando páginas já existentes. Esta seção descreve os dois procedimentos.

Para criar uma página compartilhada do zero:

1. Na página Administração de Página, selecione *Manter Páginas Compartilhadas*.

O painel Manter Páginas Compartilhadas é exibido:



2 Selecione a ação da página *Novo* (na seção inferior esquerda do painel).

Uma página compartilhada sem título e sem categoria é criada.

3 Especifique as *propriedades* da página compartilhada:

Propriedade	O que fazer

Nome do Link da Página (URI)	Especifique o nome de URI da página (como ele deve aparecer no URL da interface de usuário). Por exemplo, se você especificar o URI:
	
	`MySharedPage`
	
	ele aparecerá no URL da seguinte maneira:
	
	`http://myappserver:8080/IDM/portal/cn/`
	`MyContainerPage/`**`MySharedPage`**

Propriedade	O que fazer
Nome da Página	Especifique o nome de exibição da página. Por exemplo: `My Shared Page` Você pode clicar em **Localizar** para especificar versões localizadas deste nome para outros idiomas.
Prioridade de Navegação	Especifique uma das seguintes opções: ◆ **Nenhum** — se não houver necessidade de atribuir uma prioridade à página compartilhada. ◆ **Definir valor** — para atribuir uma prioridade a uma página compartilhada em relação a outras páginas compartilhadas. A prioridade deve ser um número inteiro entre -1 e 9999, onde -1 é a prioridade mais alta e 9999 é a mais baixa. A definição de valores de prioridade é útil quando você quer garantir uma ordem específica para a listagem das páginas por prioridade, ou se você desejar garantir determinada seleção quando houver várias páginas padrão (no caso de usuário que pertence a diversos grupos).
Página Pai	Para que esta página compartilhada seja filho de outra página compartilhada, clique em **Selecionar Pai**. Verifique se as páginas pai e filho pertencem às **mesmas categorias** (para evitar problemas de exibição). O usuário verá esse relacionamento em tempo de execução quando usar o portlet Navegação de Página Compartilhada. Na lista de páginas compartilhadas, os filhos aparecem como uma endentação abaixo dos respectivos pais. (As páginas filho não herdam conteúdo, preferências ou configurações das páginas pai. E as páginas pai não exibem automaticamente o conteúdo das páginas filho junto com seu próprio conteúdo.)

Propriedade	O que fazer
Atribuir Categorias	Selecione zero ou mais das seguintes categorias a que a página deve pertencer: ◆ Administração ◆ Gerenciamento de Diretório ◆ Geral ◆ Páginas de Convidados ◆ Gerenciamento de Informações ◆ Gerenciamento de Senhas A atribuição de categorias é útil quando você deseja assegurar a organização da listagem das páginas por categoria, ou se você pretende garantir um subconjunto apropriado quando as páginas são filtradas por categoria. **Observação:** **Páginas de Convidados** é uma categoria especial usada para identificar páginas compartilhadas que podem ser exibidas antes de o usuário efetuar login (e não após). Para obter mais informações, consulte a seção sobre o portlet Navegação de Página Compartilhada no Capítulo 15, "Sobre os portlets" na página 237.
Descrição	Digite um texto que descreva a página.

4 Clique em *Gravar Página* (na parte inferior da seção de propriedades da página).

Para criar uma página compartilhada copiando uma página já existente:

1 Na página Administração de Página, selecione *Manter Páginas Compartilhadas*.

   O painel Manter Páginas Compartilhadas é exibido (como indicado no procedimento anterior).

2 Na lista de páginas compartilhadas, *selecione* a página a ser copiada.

   Dica: Se a lista for longa, você pode *refiná-la* (por categoria ou texto inicial) para encontrar a página desejada mais facilmente.

3 Selecione a ação da página *Copiar* (na seção inferior esquerda do painel).

   Uma nova página compartilhada será criada com o nome *Cópia de NomeDePáginaOriginal*.

4 Especifique as *propriedades* da página compartilhada (como descrito no procedimento anterior).

5 Clique em *Gravar Página* (na parte inferior da seção de propriedades da página).

7.3.2 Adicionando conteúdo a uma página compartilhada

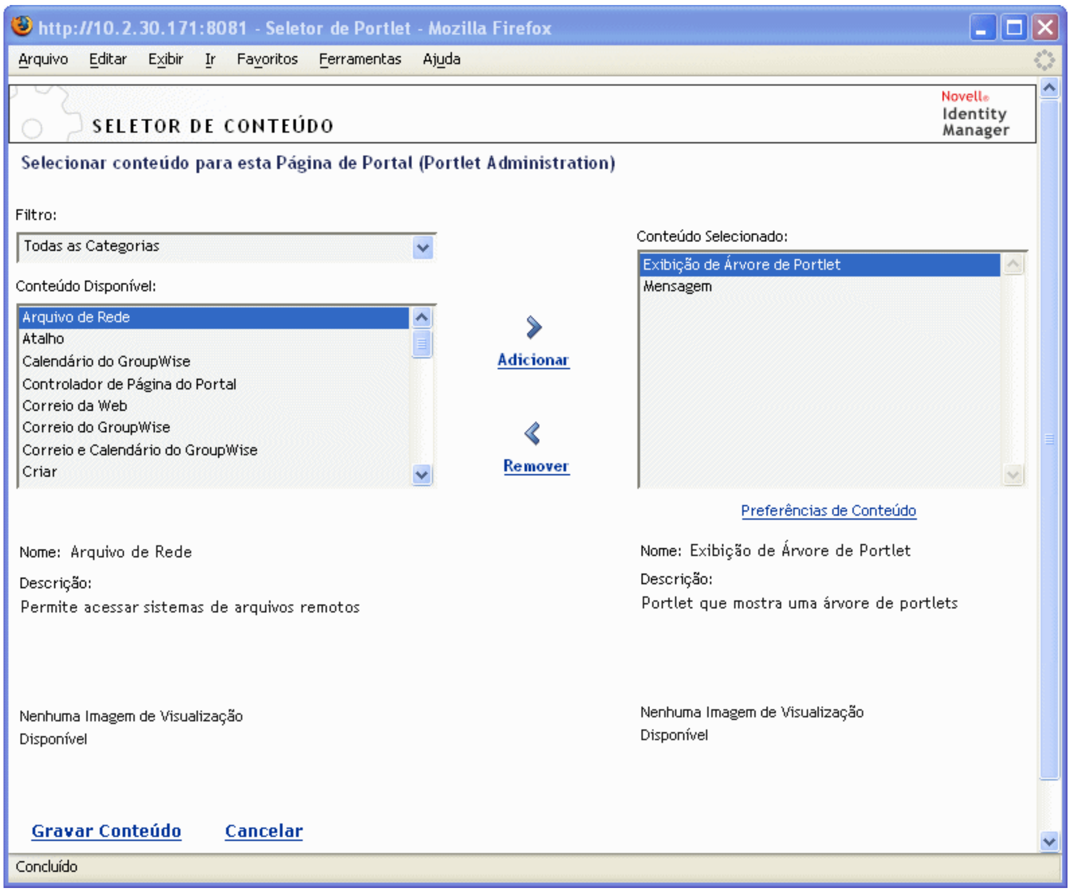
Depois de criar uma página compartilhada, a próxima etapa é adicionar conteúdo. Para isso, selecione os portlets a serem inseridos na página. Você pode usar portlets pré-elaborados que são

fornecidos com o aplicativo de usuário do Identity Manager ou outros portlets que você tenha registrado.

Para adicionar conteúdo a uma página compartilhada:

1 Abra uma página nova ou existente no painel Manter Páginas Compartilhadas e clique na tarefa da página *Selecionar Conteúdo* (na parte inferior do painel).

   O *Seletor de Conteúdo* é exibido em uma nova janela do browser:



2 Se você quiser exibir uma categoria específica de conteúdo disponível, selecione uma categoria no menu suspenso *Filtrar*.

3 Selecione um ou mais portlets na lista de *Conteúdo Disponível*.

   Dica: Mantenha a tecla *Control* pressionada para selecionar vários portlets não contíguos na lista. Use a tecla *Shift* para fazer várias seleções contíguas.

4 Clique em *Adicionar* para transferir suas escolhas para a lista de *Conteúdo Selecionado*.

5 Você pode clicar em *Preferências de Conteúdo* para editar as preferências de qualquer portlet que tenha selecionado para a página compartilhada. Os valores de preferência especificados são ativadas na instância do portlet exibida em sua página.

6 Clique em *Gravar Conteúdo*.

Depois de escolher o conteúdo da página compartilhada, você pode selecionar um novo layout, como descrito na Seção 7.3.4, “Modificando o layout de uma página compartilhada” na página 160, ou organizar o conteúdo no layout atual, como descrito na Seção 7.3.5, “Organizando conteúdo na página compartilhada” na página 161.

7.3.3 Apagando conteúdo de uma página compartilhada

No processo de criar páginas compartilhadas, para apagar conteúdo, você deve remover os portlets da página. Você pode usar o Seletor de Conteúdo ou o Seletor de Layout, como descrito nos procedimentos a seguir.

Para apagar conteúdo de uma página compartilhada usando o Seletor de Conteúdo:

1. Abra uma página no painel Manter Páginas Compartilhadas e clique na tarefa da página *Selecionar Conteúdo* (na parte inferior do painel).

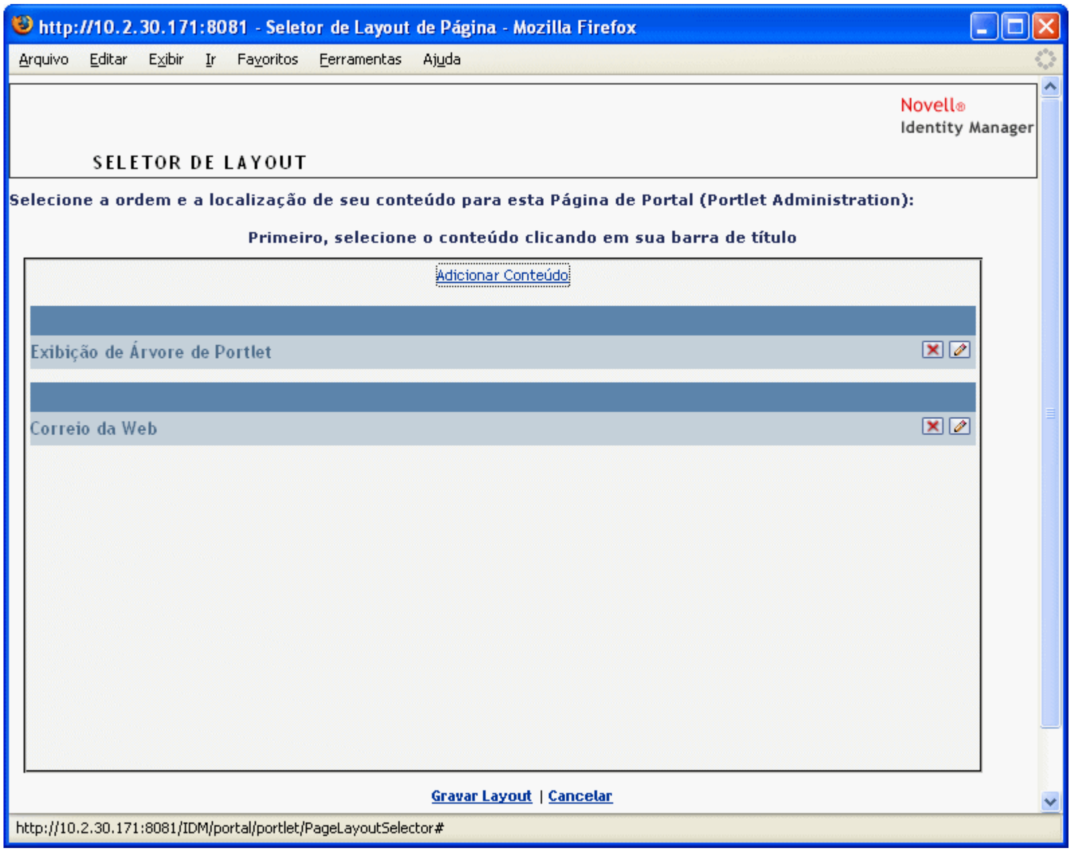
   O *Seletor de Conteúdo* é exibido em uma nova janela do browser (como indicado no procedimento anterior).
2. Na lista Conteúdo Selecionado, escolha um portlet para ser apagado e clique em *Remover*.

   O portlet é removido da página.
3. Clique em *Gravar Conteúdo*.

Para apagar conteúdo de uma página compartilhada usando o Seletor de Layout:

1. Abra uma página no painel Manter Páginas Compartilhadas e clique na tarefa da página *Organizar Conteúdo* (na parte inferior do painel).

O *Seletor de Layout* é exibido em uma nova janela do browser, mostrando os portlets dessa página:



2 Clique no botão *X* de um portlet a ser removido.

3 Ao ser solicitado, clique em *OK* para confirmar.

O portlet é removido da página.

4 Clique em *Gravar Layout*.

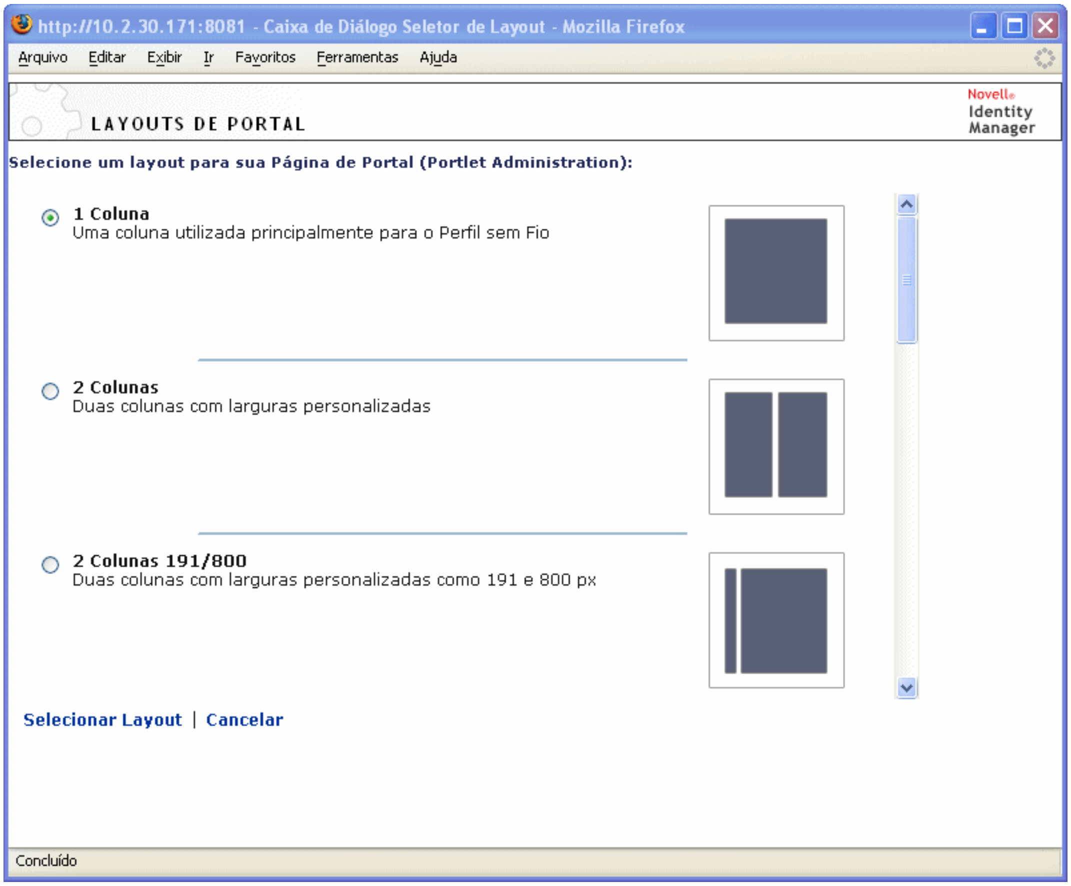
7.3.4 Modificando o layout de uma página compartilhada

Quando você modifica o layout de uma página compartilhada, o conteúdo existente é reorganizado para acomodar-se ao novo layout. Em alguns casos, pode ser necessário ajustar o resultado final.

Para modificar o layout de uma página compartilhada:

1 Abra uma página no painel Manter Páginas Compartilhadas e clique na tarefa da página *Selecionar Layout* (na parte inferior do painel).

A lista *Layouts de Portal* é exibida em uma nova janela do browser:



2 *Percorra* as opções e *selecione* o layout desejado.

3 Clique em *Selecionar Layout*.

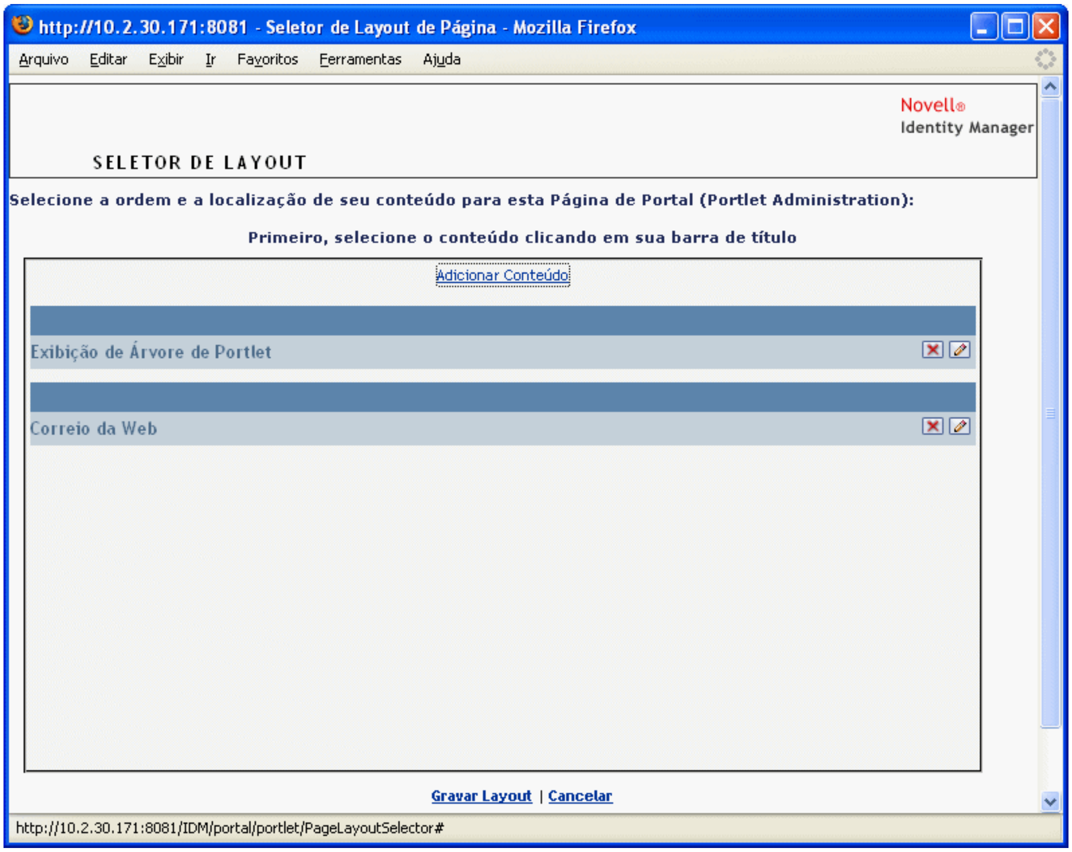
7.3.5 Organizando conteúdo na página compartilhada

Depois de designar o conteúdo e o layout da página compartilhada, você pode posicionar o conteúdo no layout, adicionar outros portlets em locais específicos ou apagar portlets.

Para organizar conteúdo em uma página compartilhada:

1 Abra uma página no painel Manter Páginas Compartilhadas e clique na tarefa da página *Organizar Conteúdo* (na parte inferior do painel).

O *Seletor de Layout* é exibido em uma nova janela do browser, mostrando os portlets dessa página:



2 Se quiser *adicionar um portlet* à página, siga estas etapas:

2a Clique em *Adicionar Conteúdo* no frame de layout desejado.

O *Seletor de Portlet* é exibido em uma nova janela do browser.

2b Se você quiser exibir uma categoria específica de conteúdo disponível, selecione uma categoria no menu suspenso *Filtrar*.

2c Selecione um portlet na lista de *Conteúdo Disponível*.

2d Clique em *Selecionar Conteúdo*.

O Seletor de Portlet fecha e o portlet selecionado aparece no frame de layout de destino do Seletor de Layout.

3 Se você quiser *mover um portlet* para outra parte do layout, siga estas etapas específicas ao browser:

Browser	O que fazer
Internet Explorer	1. Mova o cursor sobre a barra de título do portlet até ele assumir a forma de uma mão. 2. Mantenha o botão esquerdo do mouse pressionado e arraste o portlet até o local desejado no layout.

Browser	O que fazer
Mozilla	1. Clique no portlet que deseja mover. 2. Clique dentro do frame de layout de destino. O portlet é transferido.

4 Se quiser *remover um portlet* do layout, siga estas etapas:

4a Clique no botão *X* do portlet a ser removido.

4b Ao ser solicitado, clique em *OK* para confirmar.

O portlet é removido do layout.

5 Se quiser *editar as preferências* de um portlet, siga estas etapas:

5a Clique no botão de *lápis* do portlet a ser editado.

As *Preferências de Conteúdo* do portlet são exibidas no browser.

5b *Mude* os valores da preferência conforme apropriado.

Os valores de preferência especificados são ativados na instância do portlet exibida em sua página.

5c Clique em *Gravar Preferências*.

6 Clique em *Gravar Layout* para registrar as mudanças e fechar o Seletor de Layout.

7.3.6 Exibindo uma página compartilhada

Para exibir sua página, vá até o URL da página compartilhada no seu browser.

Para exibir uma página compartilhada:

- No seu *browser da Web*, vá até o seguinte URL:

```
http://server:port/IDM-war-context/portal/pg/shared-page-name
```

Por exemplo, para exibir a página compartilhada *MySharedPage*:

```
http://myappserver:8080/IDM/portal/pg/MySharedPage
```

7.4 Atribuindo permissões para as páginas

Você pode atribuir permissão a outros usuários, grupos e containers para trabalhar com páginas de container e páginas compartilhadas específicas. Dois níveis de segurança de permissão podem ser especificados:

Permissão	Descrição	Pode ser atribuída para
Exibir	Permite que um usuário, grupo ou container acesse a página e a visualize em uma lista de páginas disponíveis	**Páginas de container** e **páginas compartilhadas**
Propriedade	Permite que um usuário, grupo ou container modifique o conteúdo e o layout da página, além de atribuir a permissão Exibir e Propriedade a outros usuários, grupos e containers	**Páginas compartilhadas**

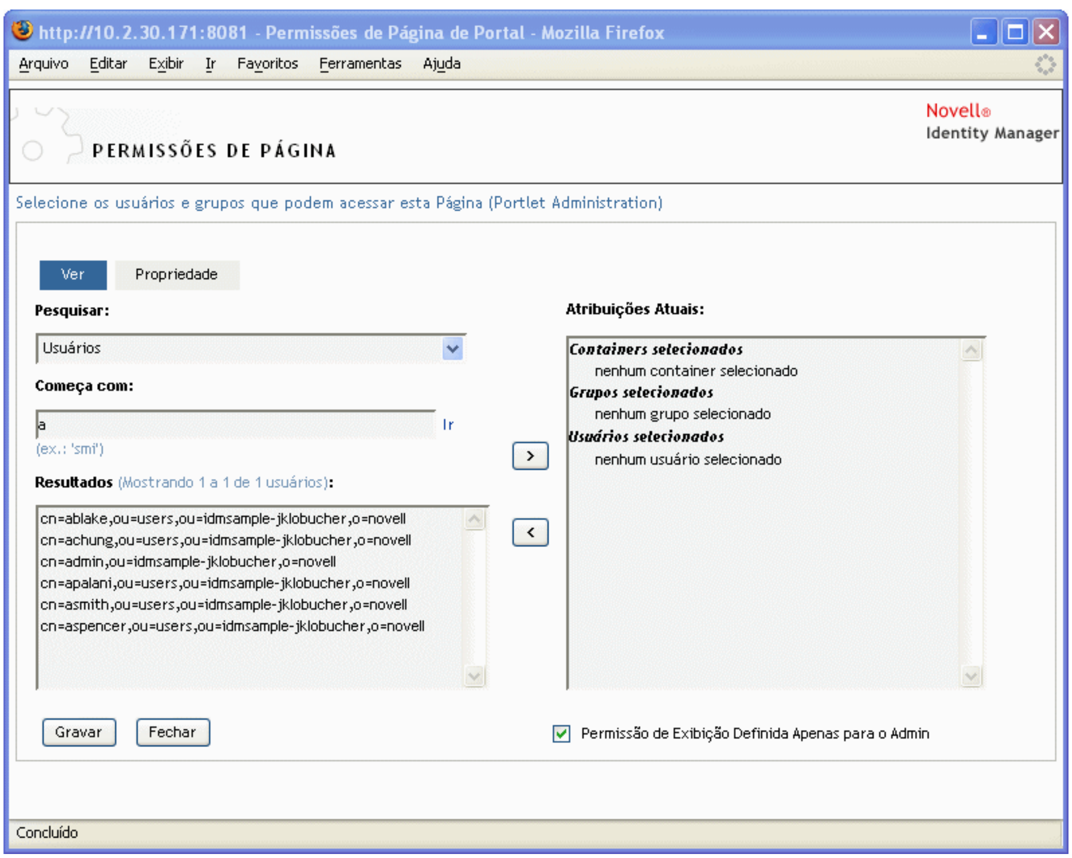
7.4.1 Atribuindo permissão para Exibir página

Quando você concede a permissão Exibir aos usuários em relação a uma página de container ou a uma página compartilhada, eles podem acessar a página e visualizá-la em uma lista de páginas disponíveis.

Para atribuir a permissão Exibir para páginas de container ou páginas compartilhadas:

1 Abra uma página no painel Manter Páginas de Container ou Manter Páginas Compartilhadas e clique na tarefa da página *Atribuir Permissões* (na parte inferior do painel).

A caixa de diálogo *Permissões de Página* é exibida em uma nova janela do browser:



2 Vá até a guia *Exibir*.

3 Especifique valores para as seguintes *configurações de pesquisa*:

Configuração	O que fazer
Pesquisar	Selecione uma das seguintes opções no menu suspenso: ◆ Usuários ◆ Grupos ◆ Containers

Começa com	Se você deseja:
	◆ **Localizar todos** os objetos disponíveis do tipo que você especificou (usuário, grupo ou container), deixe esta configuração em branco.
	◆ **Localizar um subconjunto** desses objetos, informe os caracteres iniciais dos valores CN desejados. (Não há distinção entre maiúsculas e minúsculas, nem suporte a curingas.)
	Por exemplo, a busca por grupos que começam com `S` limitam os resultados da pesquisa a algo como:
	`cn=Sales,ou=groups,o=MyOrg`
	`cn=Service,ou=groups,o=MyOrg`
	`cn=Shipping,ou=groups,o=MyOrg`
	Uma busca por grupos que começam com `Se` retorna:
	`cn=Service,ou=groups,o=MyOrg`

4 Clique em *Ir*.

Os resultados da pesquisa aparecem na lista *Resultados*.

5 *Selecione* os usuários, os grupos ou os containers que devem ser atribuídos à página e clique no botão *Adicionar* (>).

Dica: Mantenha a tecla *Control* pressionada para fazer várias seleções.

6 Habilite ou desabilite o recurso de *bloqueio de página* da seguinte maneira:

Se você deseja	Faça isto
Bloquear a página de forma que somente o Administrador do Aplicativo de Usuário possa vê-la	Marque **Permissão de Exibição Definida Apenas para o Admin**

Se você deseja	Faça isto
Permitir que todos os usuários, grupos e containers atribuídos vejam a página	Desmarque **Permissão de Exibição Definida Apenas para o Admin** **Observação:** Se você desmarcar esta configuração mas não houver usuários, grupos ou containers explicitamente atribuídos à página, **todos terão permissão Exibir** para a página.

7 Clique em *Gravar* e, em seguida, clique em *Fechar*.

7.4.2 Atribuindo proprietários de página compartilhada

Os usuários que possuem páginas compartilhadas podem modificar o conteúdo de suas páginas e mudar as preferências de portlets nessas páginas.

Para atribuir a permissão Propriedade para páginas compartilhadas:

1 Abra uma página no painel Manter Páginas Compartilhadas e clique na tarefa da página *Atribuir Permissões* (na parte inferior do painel).

   A caixa de diálogo *Permissões de Página* é exibida em uma nova janela do browser (como indicado no procedimento anterior).

2 Vá até a guia *Propriedade*.

3 Especifique valores para as seguintes *configurações de pesquisa*:

Configuração	O que fazer
Pesquisar	Selecione uma das seguintes opções no menu suspenso: ◆ Usuários ◆ Grupos ◆ Containers

Configuração	O que fazer

Começa com	Se você deseja:
	◆ **Localizar todos** os objetos disponíveis do tipo que você especificou (usuário, grupo ou container), deixe esta configuração em branco.
	◆ **Localizar um subconjunto** desses objetos, informe os caracteres iniciais dos valores CN desejados. (Não há distinção entre maiúsculas e minúsculas, nem suporte a curingas.)
	Por exemplo, a busca por grupos que começam com `S` limita os resultados da pesquisa a algo como:
	`cn=Sales,ou=groups,o=MyOrg`
	`cn=Service,ou=groups,o=MyOrg`
	`cn=Shipping,ou=groups,o=MyOrg`
	Uma busca por grupos que começam com `Se` retorna:
	`cn=Service,ou=groups,o=MyOrg`

4 Clique em *Ir*.

Os resultados da pesquisa aparecem na lista *Resultados*.

5 *Selecione* os usuários, os grupos ou os containers que devem ser atribuídos à página e clique no botão *Adicionar* (>).

Dica: Mantenha a tecla *Control* pressionada para fazer várias seleções.

6 Habilite ou desabilite o recurso de *bloqueio de página* da seguinte maneira:

Se você deseja	Faça isto
Bloquear a página de forma que somente o Administrador de Aplicativo de Usuário possa trabalhar com ela	Marque **Permissão de Propriedade Definida Apenas para o Admin**
Permitir que todos os usuários, grupos e containers atribuídos trabalhem com a página	Desmarque **Permissão de Propriedade Definida Apenas para o Admin** **Observação:** Se você desmarcar esta configuração mas não houver usuários, grupos ou containers explicitamente atribuídos à página, **todos terão permissão de Propriedade** para a página.

7 Clique em *Gravar* e, em seguida, clique em *Fechar*.

7.4.3 Permitindo o acesso do usuário à página Criar Usuário ou Grupo

Por padrão, somente Administradores do Aplicativo de Usuário podem ver e usar a página *Criar Usuário ou Grupo*, que é uma página compartilhada na *guia Auto-atendimento de Identidade* da interface de usuário do Identity Manager. Entretanto, quando apropriado, o Administrador de Aplicativo de Usuário pode *conceder permissão para que um ou mais usuários finais* também tenham acesso à página. Por exemplo, pessoas selecionadas em cargos de administração ou gerenciamento talvez precisem criar usuários, grupos ou grupos de tarefas.

Para que esses usuários tenham acesso à página Criar Usuário ou Grupo:

1 No painel *Manter Páginas Compartilhadas*, abra a página denominada *Criar Usuário ou Grupo*.

2 Use a tarefa da página *Atribuir Permissões* para conceder *permissão de Exibir* a usuários, grupos ou containers apropriados na página compartilhada Criar Usuário ou Grupo.

3 Passe de Administração de Página para *Administração de Portlet* e abra o registro de portlet chamado *CreatePortlet* (usado na página Criar Usuário ou Grupo).

4 Use o painel *Segurança* para conceder *permissões de Lista e Execução* a usuários, grupos ou containers apropriados no registro de portlet CreatePortlet.

Para obter mais informações sobre como atribuir permissões para portlet, consulte o Capítulo 9, "Administração de Portlet" na página 179.

5 Vá até o *iManager* e use uma conta de administrador para *efetuar login na árvore* do seu cofre de identidade.

6 Verifique se as pessoas que usarão Criar Usuário ou Grupo têm *Direitos de Criar para a propriedade [Direitos de Entrada]* nos container(s) em que os objetos (usuários, grupos ou grupos de tarefas) serão criados.

Por exemplo, você pode *modificar trustees* para determinado container e adicionar os usuários, grupos ou containers apropriados como trustees. Para cada trustee, você pode atribuir os seguintes direitos:

Nome da propriedade	Direitos atribuídos	Herdar
[Direitos a Todos os Atributos]	◆ Comparar ◆ Ler ◆ Gravar	Sim (marque esta caixa de seleção)
[Direitos de Entrada]	◆ Pesquisar ◆ Criar	Sim (marque esta caixa de seleção)

Se você não atribuir os direitos necessários no cofre de identidade (ou se esses direitos não puderem de alguma forma ser obtidos), o usuário final poderá receber uma *mensagem de erro* de Criar Usuário ou Grupo, como esta:

```
O usuário 'cn=mmackenzie,ou=users,ou=idmsample,o=novell' não tem
```

```
permissão para criar
'cn=MyNewGroup,ou=groups,ou=idmsample,o=novell' nem modificar
objetos relacionados.
```

Para saber como a página Criar Usuário ou Grupo é usada (pelos que podem acessá-la), consulte o *Aplicativo de Usuário do Identity Manager: Guia do Usuário*.

7.4.4 Permitindo o acesso do usuário a páginas Administração individuais

Por padrão, somente os Administradores de Aplicativo de Usuário podem acessar a *guia Administração* da interface de usuário do Identity Manager e as *páginas* contidas nessa guia (Administração de Página, Temas, Administração de Portlet, Portal, Segurança, Registro, Cache, Ferramentas). Contudo, se necessário, o Administrador de Aplicativo de Usuário pode *atribuir permissão para que um ou mais usuários* vejam e usem páginas específicas da guia Administração. Um exemplo pode ser o de um pequeno grupo de usuários que precisam mudar os temas periodicamente, embora não sejam Administradores do Aplicativo de Usuário.

Para permitir o acesso dos usuários a páginas Administração individuais:

1. No painel *Manter Páginas de Container*, abra *Página de Container de Admin*.

   Essa é a página de container usada quando você acessa a guia Administração da interface de usuário do Identity Manager.
2. Use a tarefa da página *Atribuir Permissões* para conceder *permissão de Exibir* aos usuários, grupos ou containers apropriados na página Container de Admin.
3. No painel *Manter Páginas Compartilhadas*, abra a página Administração apropriada (uma das páginas compartilhadas na categoria *Administração*).
4. Use a tarefa da página *Atribuir Permissões* para conceder *permissões de Exibição e Propriedade* aos usuários, grupos ou containers nessa página compartilhada.
5. Verifique se os usuários, grupos ou containers especificados têm *permissão de Execução para cada portlet* usado em uma página específica (se você restringiu esses portlets).

   Para obter mais informações sobre como atribuir permissões para portlet, consulte o Capítulo 9, “Administração de Portlet” na página 179.

7.5 Configurando páginas padrão para grupos

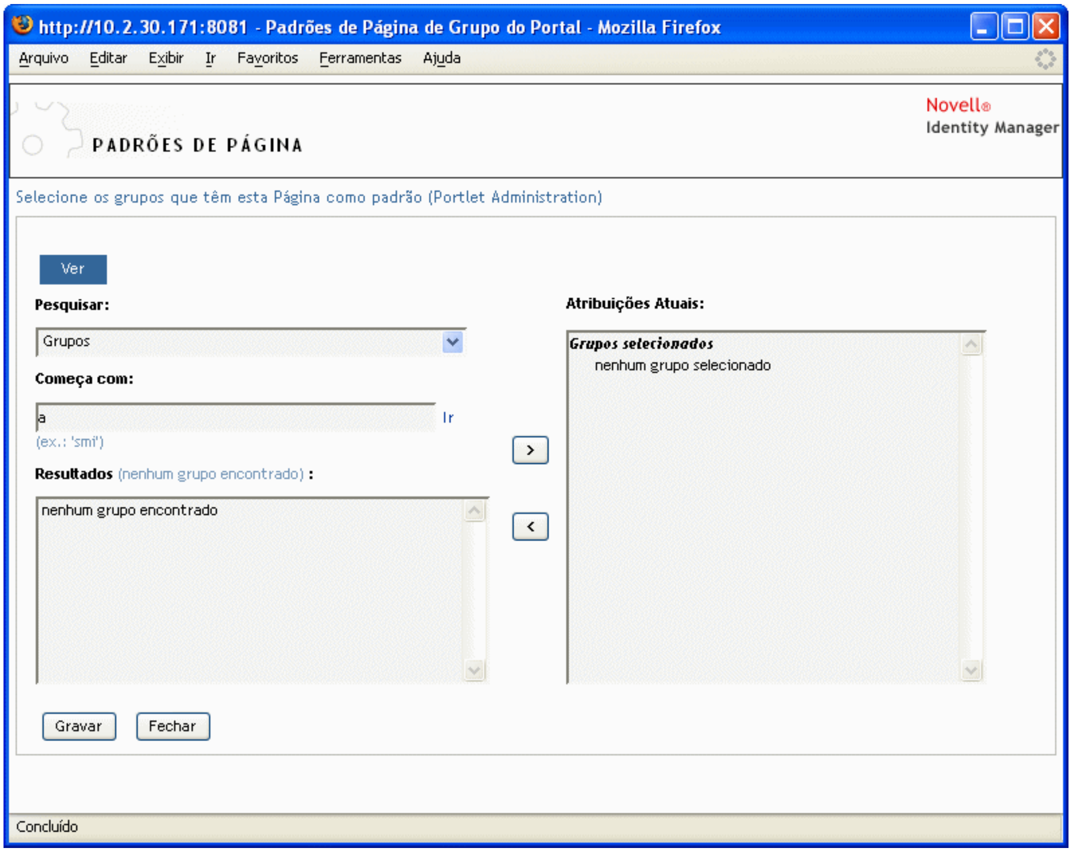
Você pode designar uma *página de container padrão* e uma *página compartilhada padrão* para qualquer grupo autorizado de usuários. Essas configurações afetam a página de container que os usuários vêem quando efetuam login e a página compartilhada que eles vêem na página de container.

Quando os usuários pertencem a diversos grupos com atribuições de página padrão, a Prioridade de Navegação é usada para determinar qual página de container e página compartilhada será exibida.

Para atribuir uma página de container padrão ou uma página compartilhada padrão a um grupo

1. Abra uma página no painel Manter Páginas de Container ou Manter Páginas Compartilhadas e clique na tarefa da página *Definir como Padrão* (na parte inferior do painel).

A caixa de diálogo *Padrões de Página* é exibida em uma nova janela do browser:



2 Especifique valores para as seguintes *configurações de pesquisa*:

Configuração	O que fazer
Pesquisar	(**Grupos** é a opção automaticamente selecionada.)

Configuração	O que fazer

Começa com	Se você deseja:
	◆ **Localizar todos** os grupos disponíveis, deixe esta configuração em branco.
	◆ **Localizar um subconjunto** desses grupos, informe caracteres iniciais dos valores CN desejados. (Não há distinção entre maiúsculas e minúsculas, nem suporte a curingas.)
	Por exemplo, a busca por grupos que começam com `S` limita os resultados da pesquisa a algo como:
	`cn=Sales,ou=groups,o=MyOrg`
	`cn=Service,ou=groups,o=MyOrg`
	`cn=Shipping,ou=groups,o=MyOrg`
	Uma busca por grupos que começam com `Se` retorna:
	`cn=Service,ou=groups,o=MyOrg`

3 Clique em *Ir*.

Os resultados da pesquisa aparecem na lista *Resultados*.

4 *Selecione* os grupos para os quais a página será um padrão e clique no botão *Adicionar* (>).

Dica: Mantenha a tecla *Control* pressionada para fazer várias seleções.

5 Clique em *Gravar* e, em seguida, clique em *Fechar*.

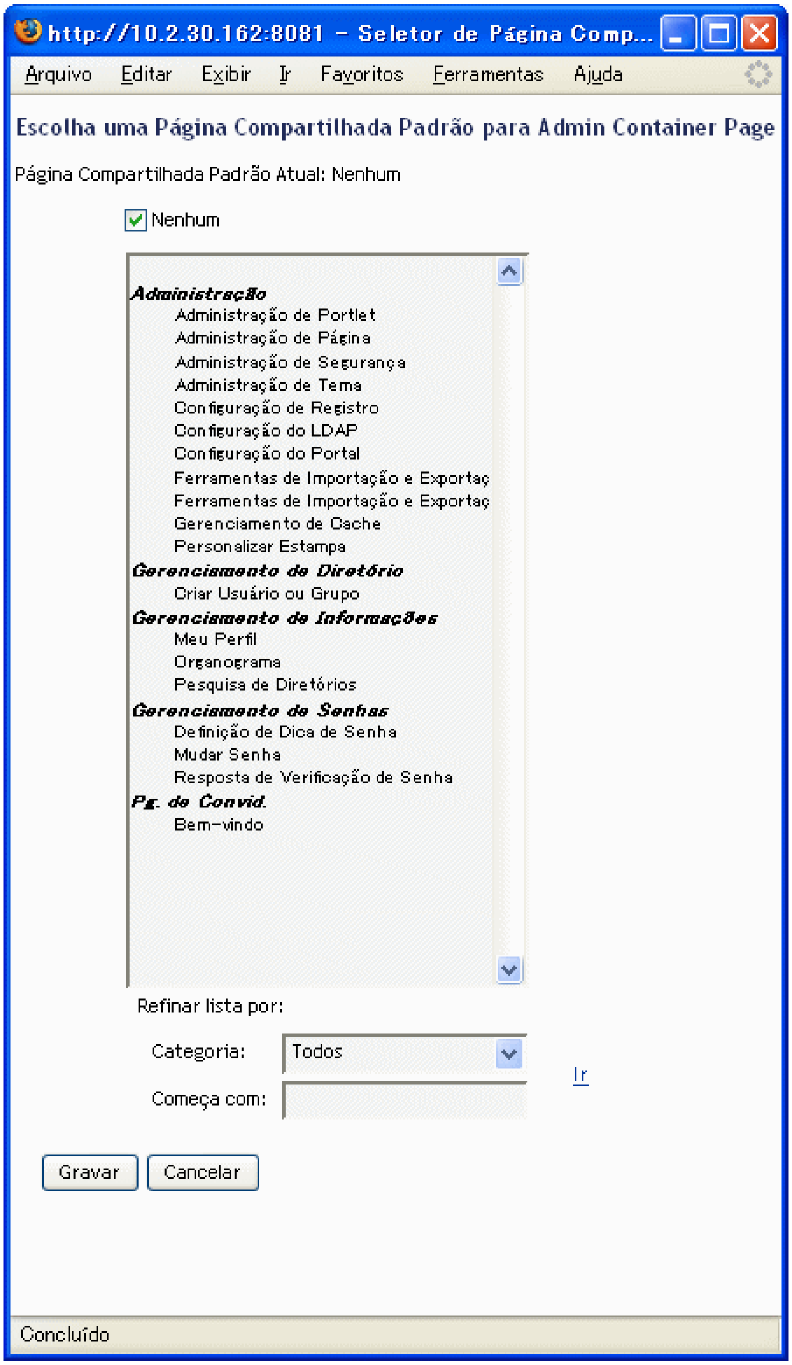
7.6 Selecionando uma página de container padrão para uma página de container

Você pode atribuir uma página compartilhada padrão a cada página de container que possui. A interface de usuário considera essa atribuição de página ao determinar o que será exibido.

Para atribuir uma página de container padrão a uma página de container:

1 Abra uma página de container no painel *Manter Páginas de Container*.
2 Na seção de propriedades da página, procure *Página Compartilhada Padrão* e clique em *Selecionar Padrão*.

A caixa de diálogo *Escolha uma Página Compartilhada Padrão* é exibida em uma nova janela do browser:



3 Se a lista de páginas compartilhadas for muito longa, você poderá *refiná-la* (por categoria ou texto inicial) para encontrar facilmente a página desejada.

4 *Selecione* uma página compartilhada para ser usada como o padrão da página de container (ou marque *Nenhum* para não ter qualquer padrão).

5 Clique em *Gravar* para aceitar a seleção e feche a caixa de diálogo.

6 Clique em *Gravar Página* (na parte inferior da seção de propriedades da página).

Configuração de tema

8

Este capítulo ensina a usar a página *Temas* da *guia Administração* da interface de usuário do Identity Manager. Os tópicos incluem:

Para obter informações gerais sobre como acessar e trabalhar com a guia Administração, consulte o Capítulo 6, “Usando a guia Administração” na página 131.

8.1 Sobre a configuração de tema

Você pode usar a página Temas para controlar a aparência da interface de usuário do Identity Manager.

Tema é um conjunto de características visuais que se aplicam a toda a interface de usuário (inclusive as páginas de convidados e de login, a guia Auto-atendimento da Proteção, a guia Solicitações e Aprovações, e a guia Administração). Sempre há um tema ativado na interface de usuário. A página Temas contém uma variedade de temas caso você queira mudar para algum outro.

Na página Temas, também é possível:

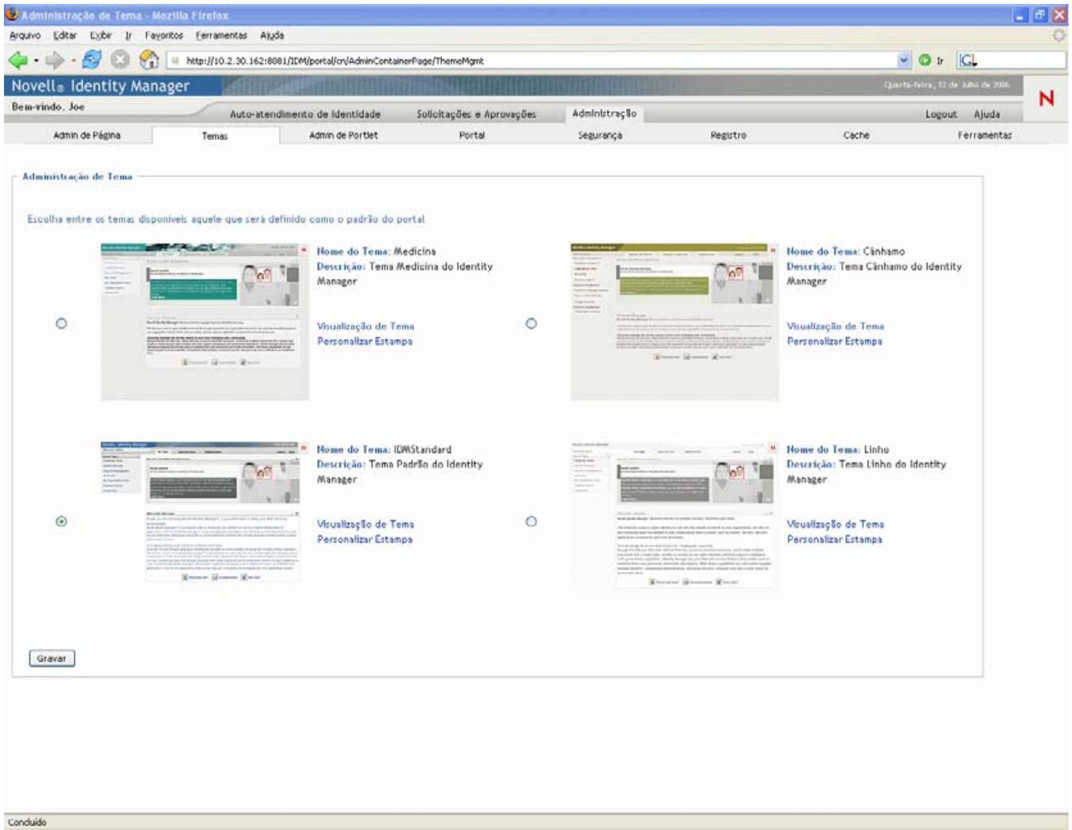
- *Visualizar* cada opção de tema para ver sua aparência
- *Personalizar* toda opção de tema para que ela reflita sua própria marca (logotipo, entre outros)

8.2 Visualizando um tema

Antes de escolher um tema, você pode visualizar como ele afetará a aparência da interface de usuário do Identity Manager.

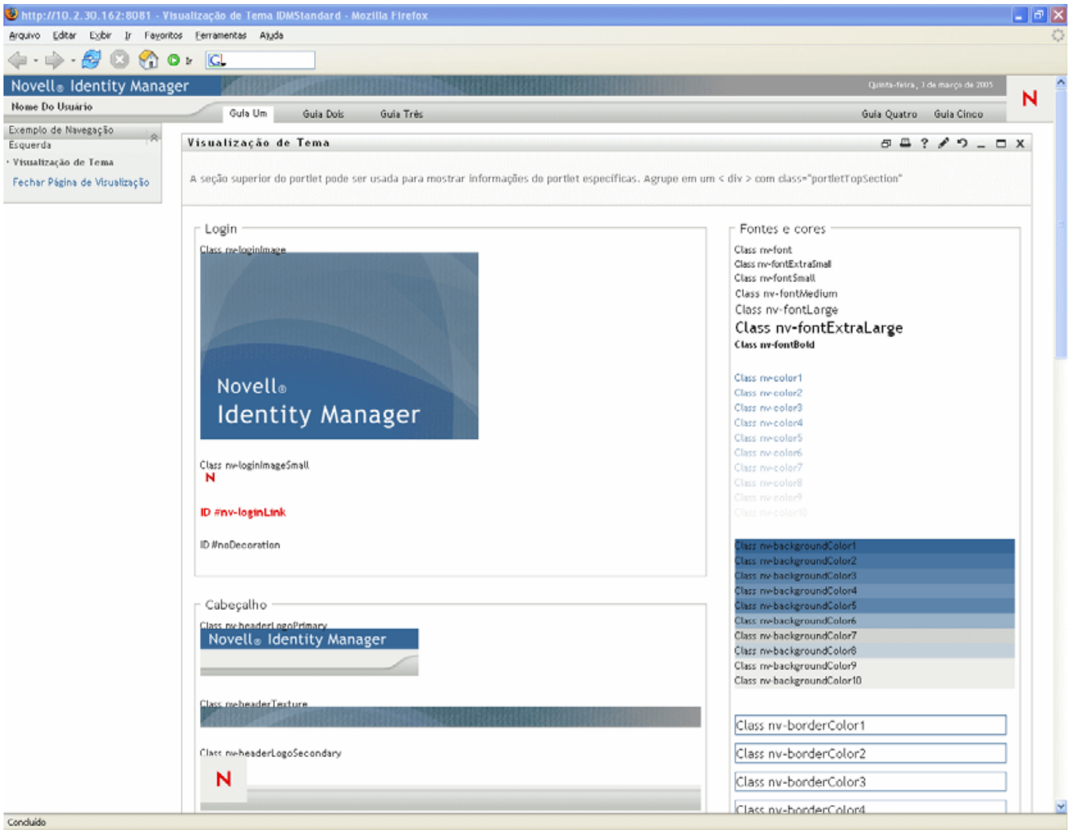
Para visualizar um tema:

1 Vá até a página *Temas*:



2 Encontre um tema de seu interesse e clique no link *Visualização de Tema* correspondente.

Você visualiza o tema em uma nova janela do browser:



3 *Role* a visualização para ver as características do tema.

4 Quando terminar, clique em *Fechar Página de Visualização* (no canto superior esquerdo) ou feche a janela de visualização manualmente.

8.3 Escolhendo um tema

Quando você encontra um tema de seu agrado, pode optar por torná-lo o *tema atual* da interface de usuário do Identity Manager.

Para escolher um tema:

1 Vá até a página *Temas*.

2 Clique no *botão de opção* do tema desejado.

3 Clique no botão *Gravar*.

A aparência da interface de usuário muda de acordo com o tema escolhido.

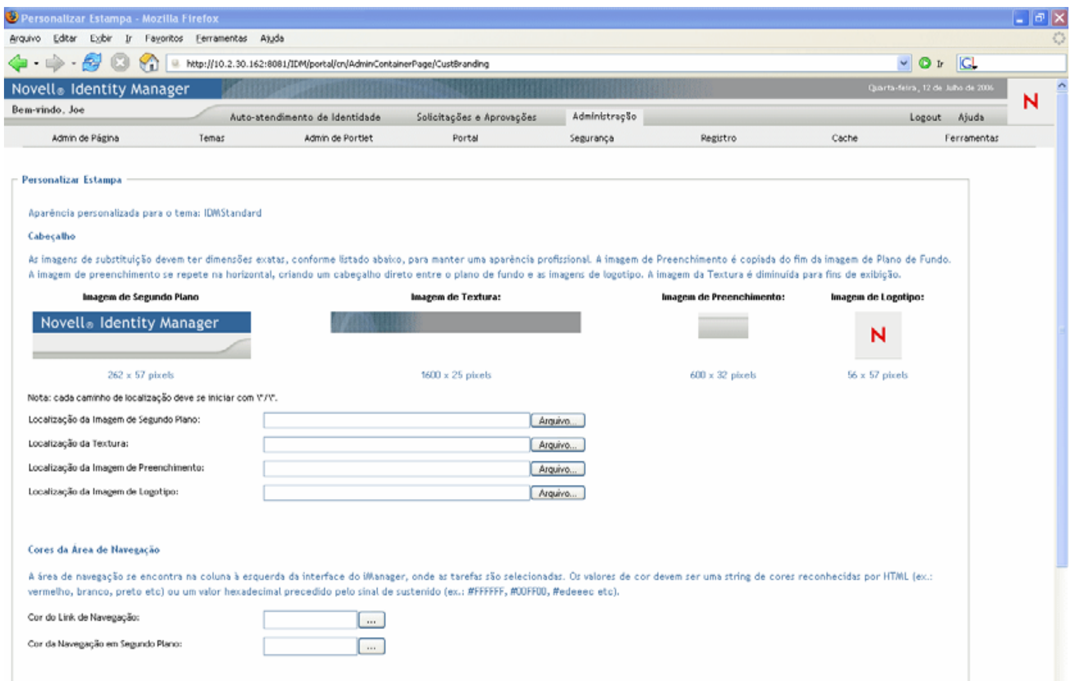
8.4 Personalizando um tema

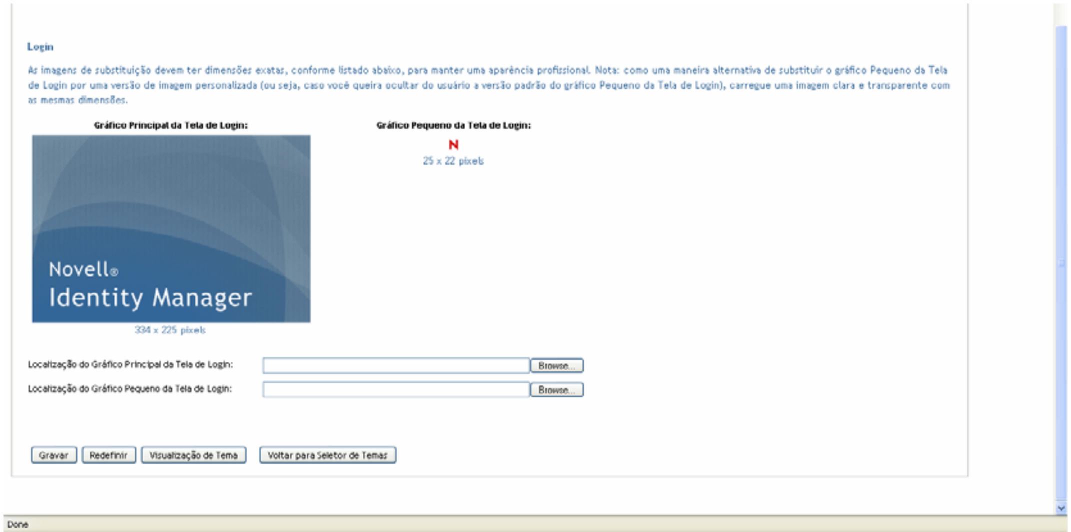
Para ajustar um tema, você o substitui pelas suas próprias *imagens* e muda algumas *configurações de cor*. Esse procedimento confere à interface de usuário do Identity Manager uma aparência personalizada que atende às exigências particulares de sua empresa.

Para personalizar um tema:

1. Vá até a página *Temas*.
2. Encontre um tema que você queira ajustar e clique no link *Personalizar Estampa* correspondente.

   A página Temas exibe as configurações de Personalizar Estampa do tema em questão.





3 Especifique *suas personalizações* nas configurações (conforme necessário), inclusive:

- Imagens de cabeçalho
- Cores da área de navegação
- Imagens de login

Siga as instruções na tela para especificar cada configuração.

4 Clique no botão *Gravar*.

Se você estiver editando o tema atual, a aparência da interface de usuário mudará de acordo com as suas personalizações. (Para desfazer todas as personalizações realizadas no tema, clique no botão *Redefinir*.)

Observação: O botão *Visualização de Tema* fica disponível enquanto você efetua as personalizações. Entretanto, lembre-se de que ele sempre exibe as *características originais* do tema. Suas mudanças não são exibidas.

---

5 Depois de trabalhar no tema, clique no botão *Voltar para Seletor de Temas*.

Administração de Portlet

9

Este capítulo informa como usar a página *Administração de Portlet* da guia *Administração* da interface de usuário do Identity Manager. Os tópicos incluem:

Para obter informações gerais sobre como acessar e trabalhar com a guia Administração, consulte o Capítulo 6, "Usando a guia Administração" na página 131.

9.1 Sobre a administração de portlet

Você pode usar a página Administração de Portlet para controlar os *portlets* disponíveis na interface de usuário do Identity Manager e quem tem permissão para acessá-los. Os portlets são elementos conectáveis da interface de usuário (com base em um *padrão Java*) que fornece o conteúdo das páginas da interface de usuário (incluindo as páginas de container e as páginas compartilhadas).

O gerenciamento de portlets envolve o trabalho com os seguintes elementos:

Com o que você trabalha	Descrição
Aplicativos de portlet	WARs compatíveis com o Java Portlet 1.0 que contêm o descritor de distribuição de portlet.xml e, opcionalmente, outros artefatos de tempo de execução de portlet. Consulte a Seção 9.2, "Administrando aplicativos de portlet" na página 180.)
Definições de portlet	Descritores (lêem em portlet.xml) que especificam os parâmetros de configuração do portlet. Existe uma definição para cada portlet em um aplicativo. Consulte a Seção 9.3, "Administrando definições de portlet" na página 183.)
Registros de portlet	Registros de portlets, baseados nas respectivas definições. Pode haver diversos registros do mesmo portlet em um aplicativo de portlet. Consulte a Seção 9.4, "Administrando portlets registrados" na página 187.)

Para obter detalhes sobre os portlets fornecidos com a interface de usuário do Identity Manager, consulte Parte IV, "Referência de portlet" na página 235. Para saber como usar portlets em páginas de container e páginas compartilhadas, consulte o Capítulo 7, "Administração de Página" na página 137.

9.2 Administrando aplicativos de portlet

Quando o aplicativo de usuário do Identity Manager é instalado, o arquivo *IDM.war* é distribuído no servidor de aplicativos e automaticamente registrado como um aplicativo de portlet. O arquivo IDM.war (que pode ser renomeado durante a instalação) inclui todos os portlets usados na configuração padrão da interface de usuário do Identity Manager. Ele também inclui alguns portlets adicionais que não são usados por padrão. (Os portlets IDM.war estão descritos em Parte IV, "Referência de portlet" na página 235.)

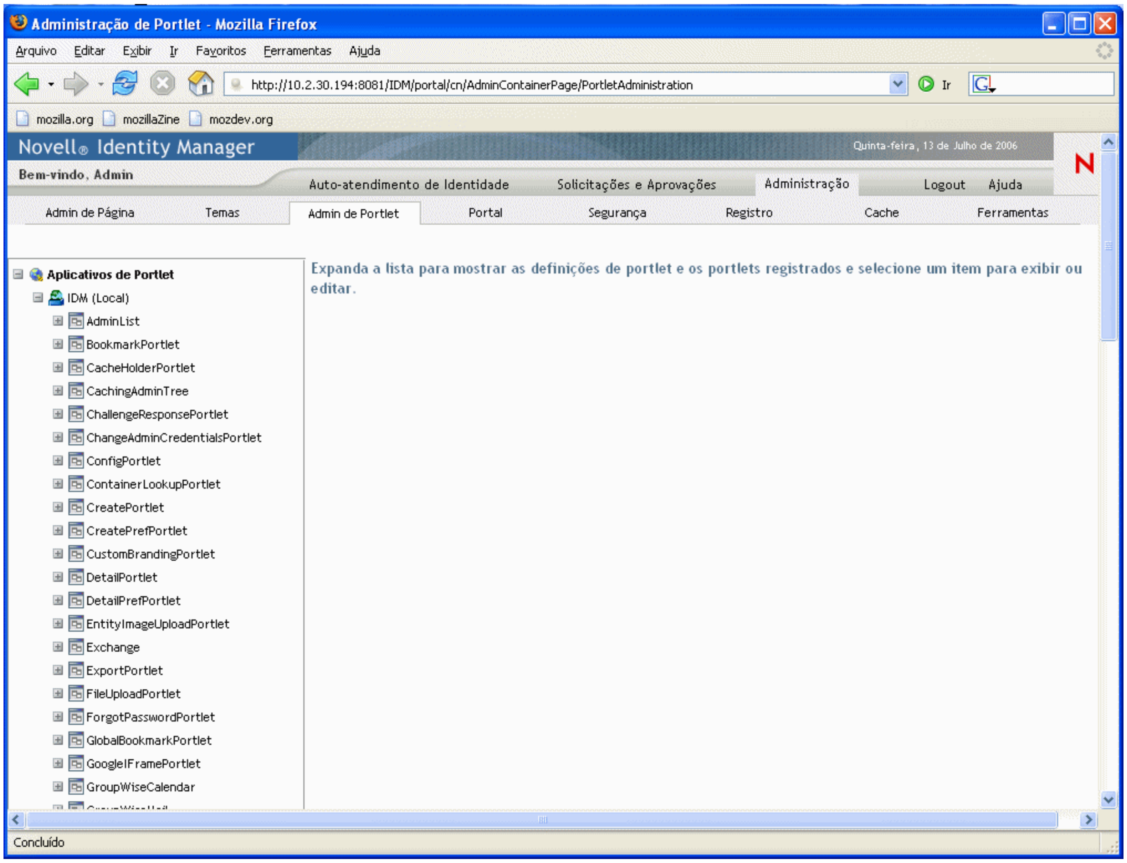
Você não está restrito aos portlets de IDM.war. Se você distribuir qualquer outro *aplicativo de portlet padrão* (WARs compatíveis com Java Portlet 1.0) em seu servidor de aplicativos, poderá trabalhar com esses aplicativos de portlet e respectivos portlets na interface de usuário do Identity Manager. Por exemplo, você verá esses aplicativos de portlet relacionados com o IDM.war na página Administração de Portlet.

A página Administração de Portlet permite que você *administre o IDM.war e outros aplicativos de portlet* das seguintes maneiras:

9.2.1 Acessando aplicativos de portlet no servidor

Quando você acessa a página Administração de Portlet, ela automaticamente *exibe uma lista* dos aplicativos de portlet (IDM.war e outros) que estão no seu servidor de aplicativos. Essa lista aparece

à esquerda como uma árvore e pode ser *expandida e pesquisada* para que você possa administrar um aplicativo de portlet selecionado e seu conteúdo:



9.2.2 Visualizando informações sobre aplicativos de portlet

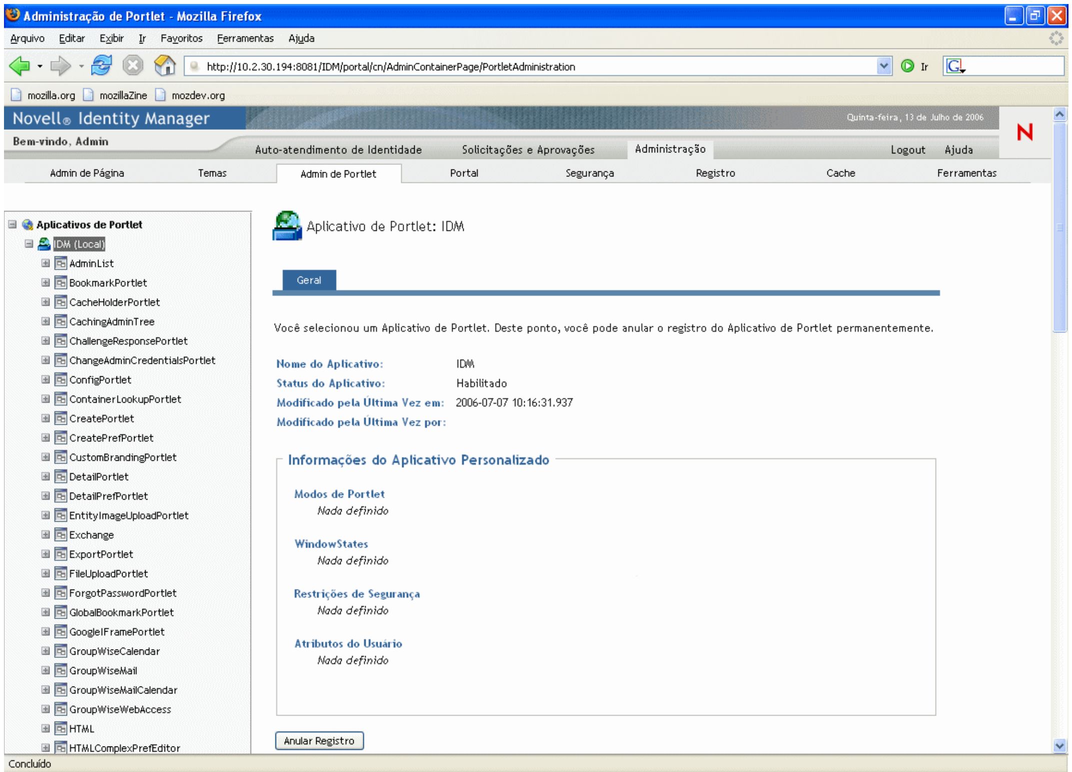
Você pode ver as seguintes informações apenas leitura sobre um aplicativo de portlet da lista:

- Nome
- Status (habilitado ou desabilitado)
- Data da última modificação
- Usuário que fez a última modificação no aplicativo
- Informações do aplicativo personalizado (se houver): modos do portlet, estados de janela, restrições de segurança e atributos do usuário

Para ver informações sobre um aplicativo de portlet:

- Na lista Aplicativos de Portlet, *selecione* o aplicativo de portlet sobre o qual você deseja se informar.

É exibido um painel *Geral* à direita, com informações sobre o aplicativo de portlet selecionado:



9.2.3 Anulando o registro de aplicativos de portlet

Se você quiser remover um aplicativo de portlet do servidor de aplicativos, deverá *anular o registro* do aplicativo de portlet antes de desfazer sua distribuição. Caso contrário, o aplicativo de portlet será redistribuído automaticamente quando o servidor reiniciar.

Quando você anula o registro de um aplicativo de portlet, todas as preferências e configurações relacionadas são removidas do banco de dados que armazena os dados do aplicativo.

Observação: Não é possível anular o registro do container de portlet *local*, que é um aplicativo de portlet local no portal. O container de portlet local gerencia os portlets contidos no portal (aplicativo de usuário do Identity Manager).

Para anular o registro de aplicativos de portlet:

1 Na lista Aplicativos de Portlet, *selecione* o aplicativo de portlet cujo registro você deseja anular.

Um painel *Geral* é exibido à direita (como indicado no procedimento anterior).

2 Clique em *Anular Registro*.

Uma janela de confirmação é exibida.

3 Clique em *OK* para confirmar a ação.

Quando o processo estiver concluído, o aplicativo de portlet cujo registro foi anulado será removido da lista Aplicativos de Portlet.

4 Para remover o aplicativo de portlet do servidor de aplicativos, use as ferramentas do servidor para *desfazer a distribuição do arquivo* que contém o aplicativo de portlet.

Observação: Para renovar o registro de um aplicativo de portlet cujo registro tenha sido anulado, é preciso *redistribuí-lo*.

9.3 Administrando definições de portlet

A página Administração de Portlet permite que você execute as seguintes tarefas relacionadas às *definições de portlet*:

- Seção 9.3.1, "Acessando definições de portlet no aplicativo de portlet distribuído" na página 183
- Seção 9.3.2, "Registrando definições de portlet" na página 184
- Seção 9.3.3, "Vendo informações sobre definições de portlet" na página 185

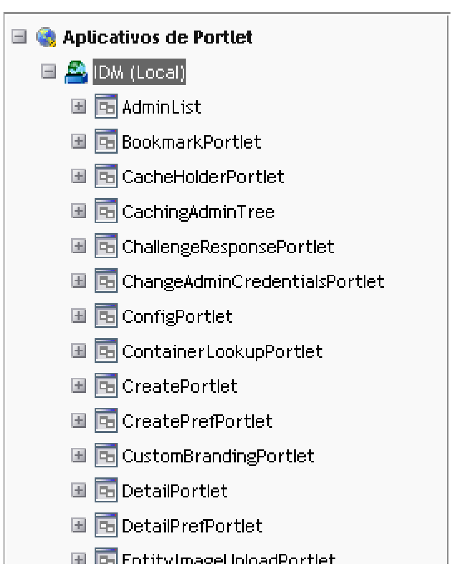
9.3.1 Acessando definições de portlet no aplicativo de portlet distribuído

A lista Aplicativos de Portlet mostra as definições de portlet no aplicativo de portlet selecionado.

Para acessar definições de portlet no aplicativo de portlet distribuído:

- Na lista Aplicativos de Portlet, *expanda* o aplicativo de portlet cujas definições de portlet você deseja acessar.

  A árvore exibe todas as definições de portlet no aplicativo de portlet em questão:



9.3.2 Registrando definições de portlet

Antes de usar um portlet, é preciso registrar essa definição com o portal (aplicativo de usuário do Identity Manager). Uma definição de portlet registrada é um *registro de portlet*. Você pode criar vários registros para um portlet, o que lhe permite colocar diversas instâncias do portlet na mesma página.

O registro de portlet herda todas as *preferências e configuração* da classe de portlet, mas você pode modificar esses valores das seguintes maneiras:

- *Ao registrar* a definição de portlet — consulte a Seção 9.4, “Administrando portlets registrados” na página 187
- *Ao adicionar uma instância* do portlet a uma página — consulte o Capítulo 7, “Administração de Página” na página 137

Todos os portlets fornecidos com o aplicativo de usuário do Identity Manager são *registrados automaticamente*.

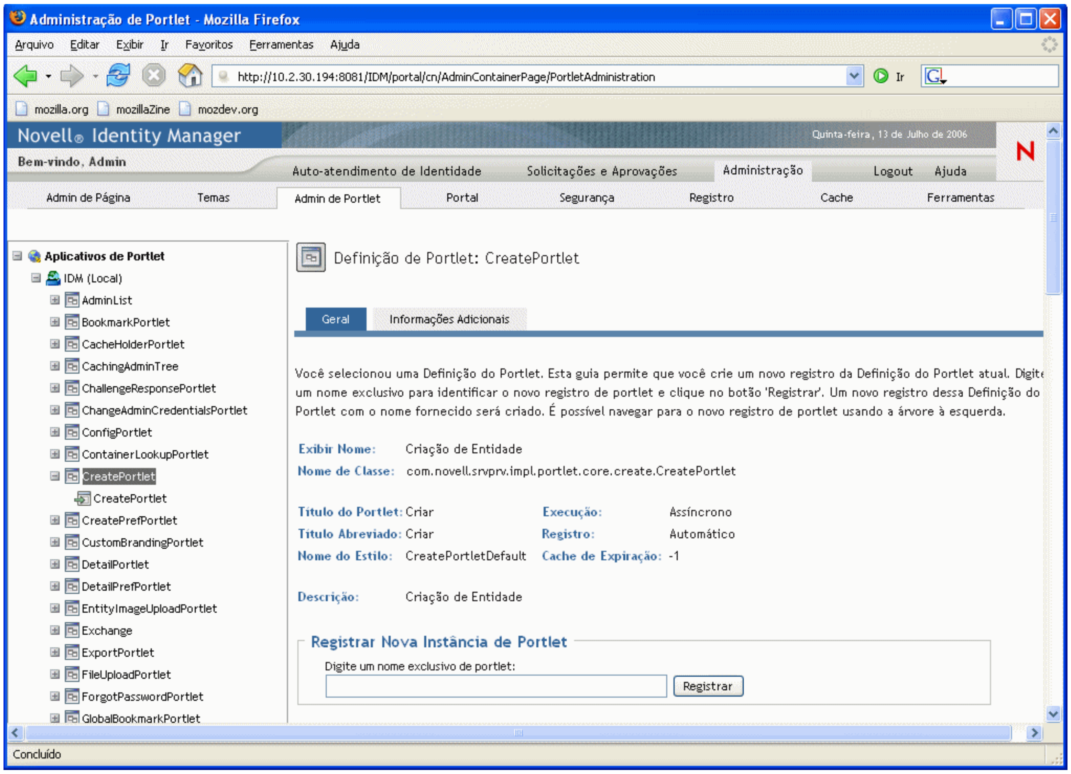
Modo de edição Se a definição de portlet tiver um modo de edição, o usuário final poderá modificar preferências específicas do registro de portlet em tempo de execução, de acordo com a lógica do método doEdit() do portlet.

O aplicativo de usuário do Identity Manager também oferece uma implementação padrão para o modo de edição. Se o método doEdit() não for implementado explicitamente, será exibida uma folha de preferências padrão.

Para registrar uma definição de portlet:

1 Na lista Aplicativos de Portlet, *selecione* a definição de portlet para a qual você deseja criar um registro.

Um painel *Geral* é exibido à direita (como indicado no procedimento anterior).



Lembre-se de que todos os *registros existentes* do portlet selecionado são relacionados na árvore Aplicativos de Portlet (à esquerda), sob o nome de definição de portlet correspondente.

2 Na caixa de texto *Registrar Nova Instância de Portlet*, especifique um nome exclusivo para o registro de portlet e clique em *Registrar*.

O novo registro de portlet é criado e relacionado na árvore Aplicativos de Portlet.

3 Para modificar as preferências e as configurações do novo registro de portlet, consulte a Seção 9.4, “Administrando portlets registrados” na página 187.

9.3.3 Vendo informações sobre definições de portlet

Você pode ver as seguintes informações apenas leitura sobre uma definição de portlet da lista:

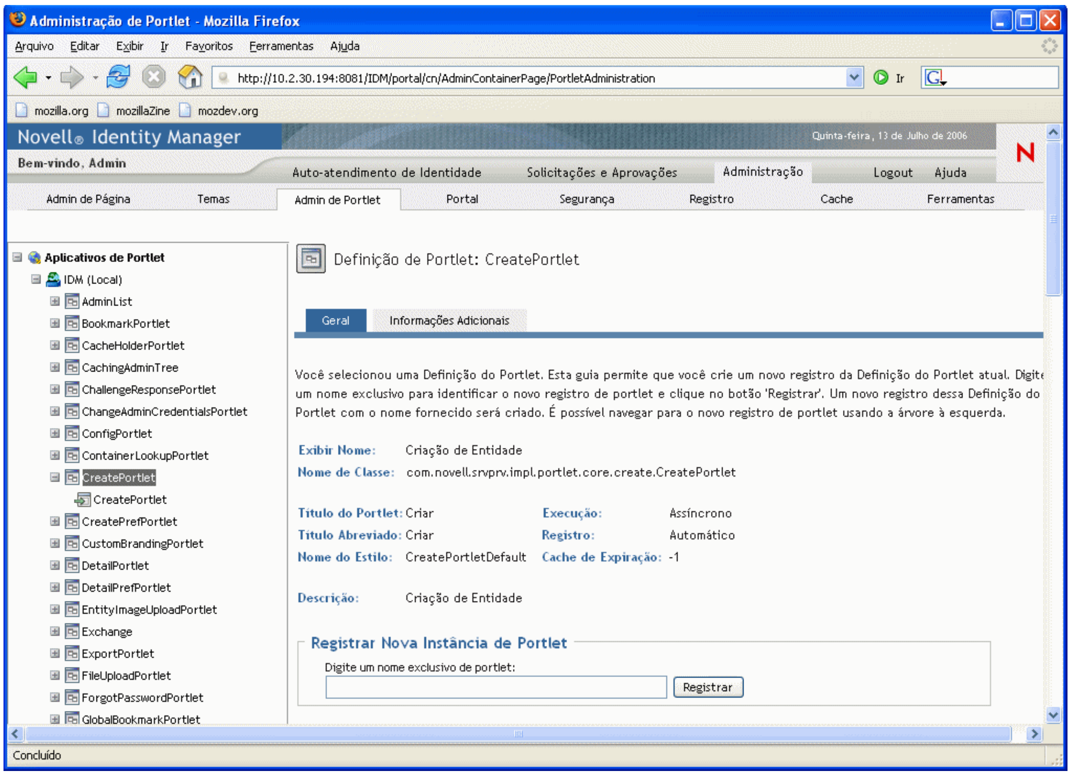
- Nome de exibição
- Nome de classe
- Título do portlet
- Tipo de execução (síncrona ou assíncrona)
- Título abreviado
- Tipo de registro
- Nome do estilo
- Tempo de expiração de cache

- Descrição
- Parâmetros de inicialização
- Palavras-chave
- Tipos mime suportados
- Modos suportados pelo portlet
- Locais suportados
- Dispositivos suportados
- Funções de segurança

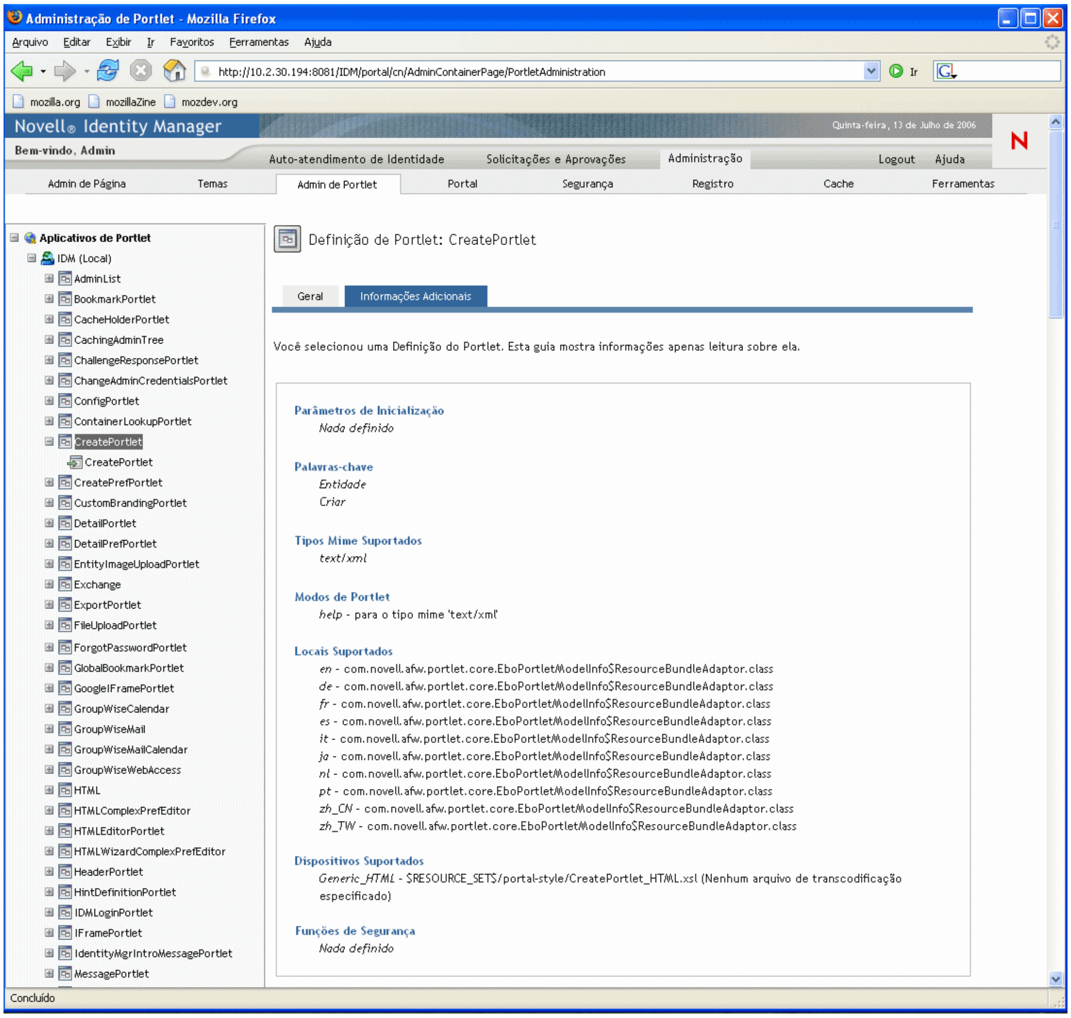
Para ver informações sobre definições de portlet:

1 Na lista Aplicativos de Portlet, *selecione* a definição de portlet sobre a qual você deseja se informar.

É exibido um painel *Geral* à direita, com informações sobre a definição de portlet selecionada:



2 Vá até o painel *Informações Adicionais* para ver mais detalhes sobre a definição de portlet selecionada:



9.4 Administrando portlets registrados

A página Administração de Portlet permite que você execute as seguintes tarefas relacionadas aos *registros de portlet*:

- Seção 9.4.1, "Acessando registros de portlet no aplicativo de portlet distribuído" na página 188
- Seção 9.4.2, "Visualizando informações sobre registros de portlet" na página 189
- Seção 9.4.3, "Designando categorias a registros de portlet" na página 189
- Seção 9.4.4, "Modificando configurações de registros de portlet" na página 190
- Seção 9.4.5, "Modificando preferências de registros de portlet" na página 193
- Seção 9.4.6, "Atribuindo permissões de segurança a registros de portlet" na página 194
- Seção 9.4.7, "Anulando o registro de um portlet" na página 197

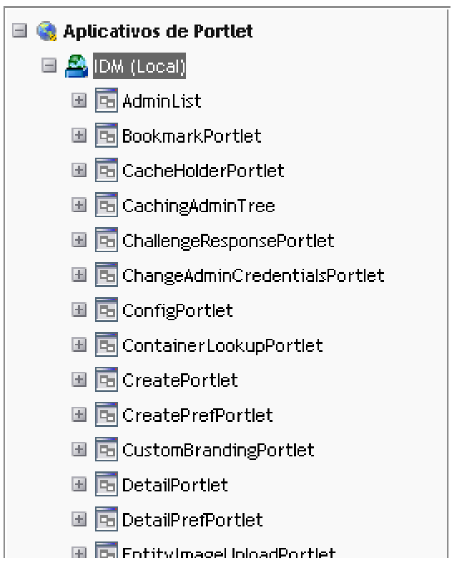
9.4.1 Acessando registros de portlet no aplicativo de portlet distribuído

A lista Aplicativos de Portlet mostra os registros de cada definição portlet em um aplicativo de portlet selecionado.

Para acessar registros de portlet no aplicativo de portlet distribuído:

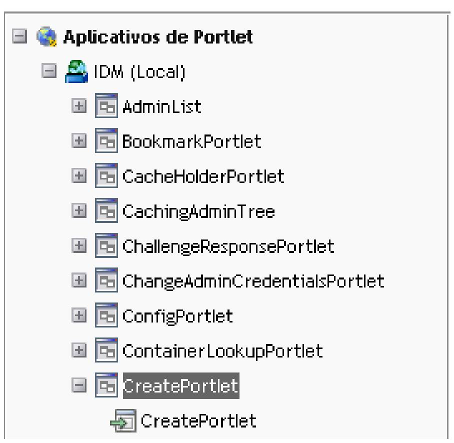
1 Na lista Aplicativos de Portlet, *expanda o aplicativo de portlet* cujos registros e definições de portlet você deseja acessar.

A árvore exibe todas as definições de portlet no aplicativo de portlet em questão:



2 *Expanda a definição de portlet* cujos registros você deseja acessar.

A árvore exibe todos os registros de portlet na definição de portlet em questão:



9.4.2 Visualizando informações sobre registros de portlet

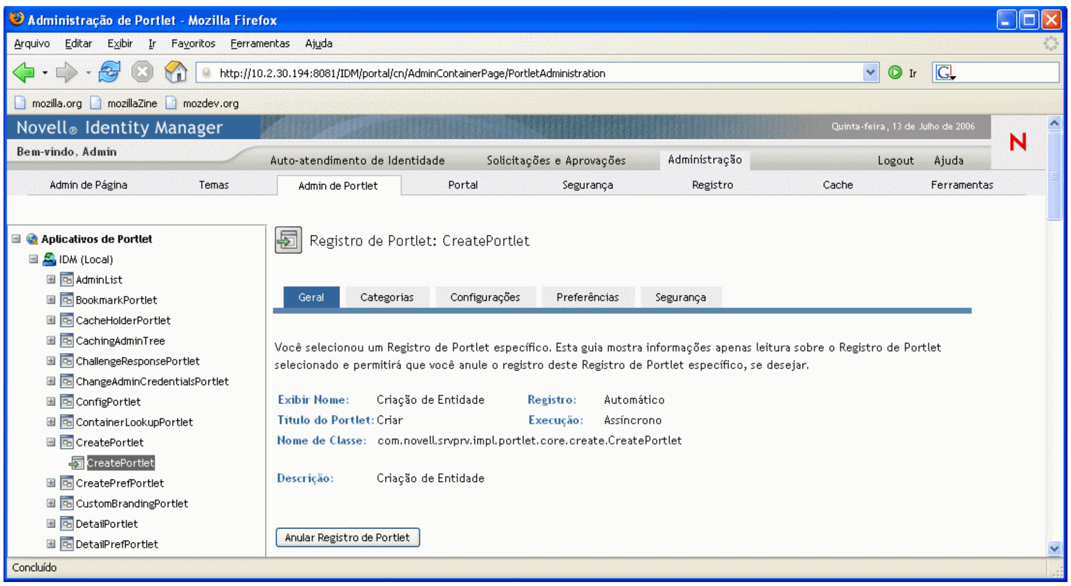
Você pode ver as seguintes informações apenas leitura sobre um registro de portlet da lista:

- Nome de exibição
- Tipo de registro
- Título do portlet
- Tipo de execução (síncrona ou assíncrona)
- Nome de classe
- Descrição

Para visualizar informações sobre registros de portlet:

- Na lista Aplicativos de Portlet, *selecione* o registro de portlet sobre o qual você deseja se informar.

  É exibido um painel *Geral* à direita, com informações sobre o registro de portlet selecionado:



9.4.3 Designando categorias a registros de portlet

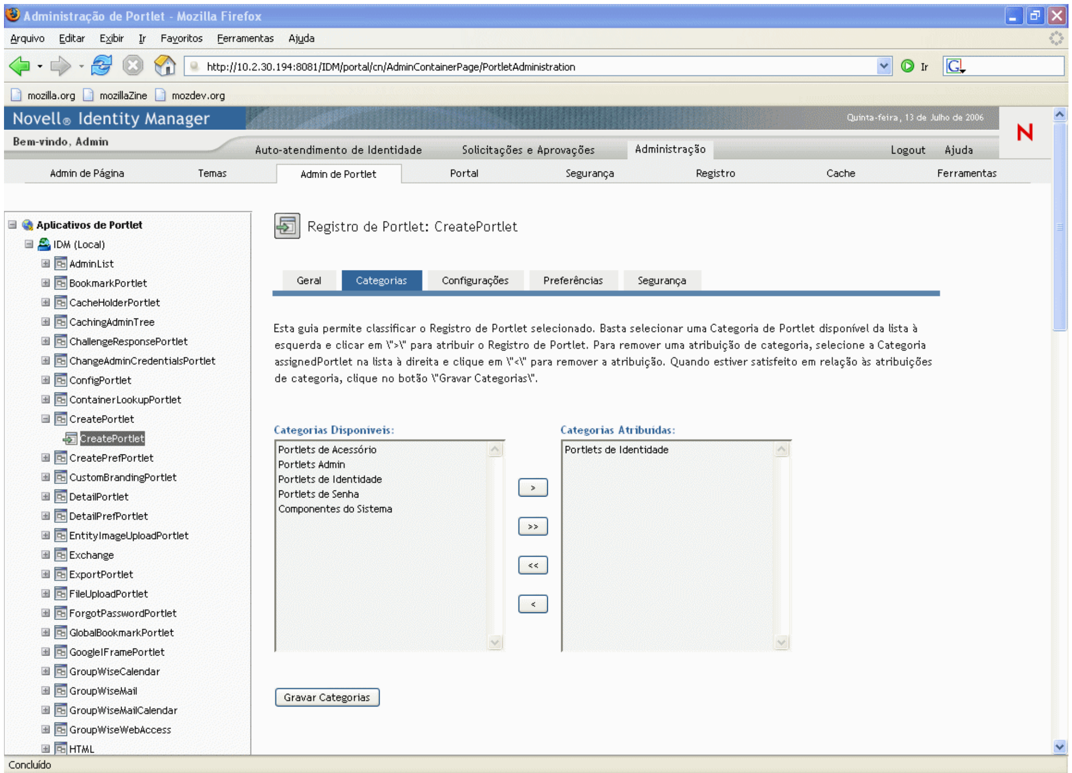
Para facilitar a busca por portlets específicos em um aplicativo de portlet, você pode organizar os registros de portlet por categoria.

Para designar categorias a registros de portlet:

1. Na lista Aplicativos de Portlet, *selecione* o registro de portlet que você deseja categorizar.

   Um painel *Geral* é exibido à direita.
2. Vá até o painel *Categorias*.

Esse painel exibe listas de categorias disponíveis e designadas para o registro de portlet selecionado.



3 Atualize a lista *Categorias Atribuídas* conforme apropriado:

Se você deseja	Faça isto
Designar uma ou mais categorias ao registro de portlet	Selecione cada categoria a ser designada e clique em >
Designar todas as categorias ao registro de portlet	Clique em >>
Remover uma ou mais designações de categoria	Selecione cada categoria a ser removida e clique em <
Remover todas as atribuições de categoria	Clique em <<

4 Clique em *Gravar Categorias*.

9.4.4 Modificando configurações de registros de portlet

As configurações de portlet definem como o portal (aplicativo de usuário do Identity Manager) interage com portlets individuais. Cada portlet é definido com estas configurações:

- Título
- Tempo de espera máximo

* Requer autenticação
* Mostrar barra de título
* Oculto ao usuário
* Opções definidas no aplicativo de portlet

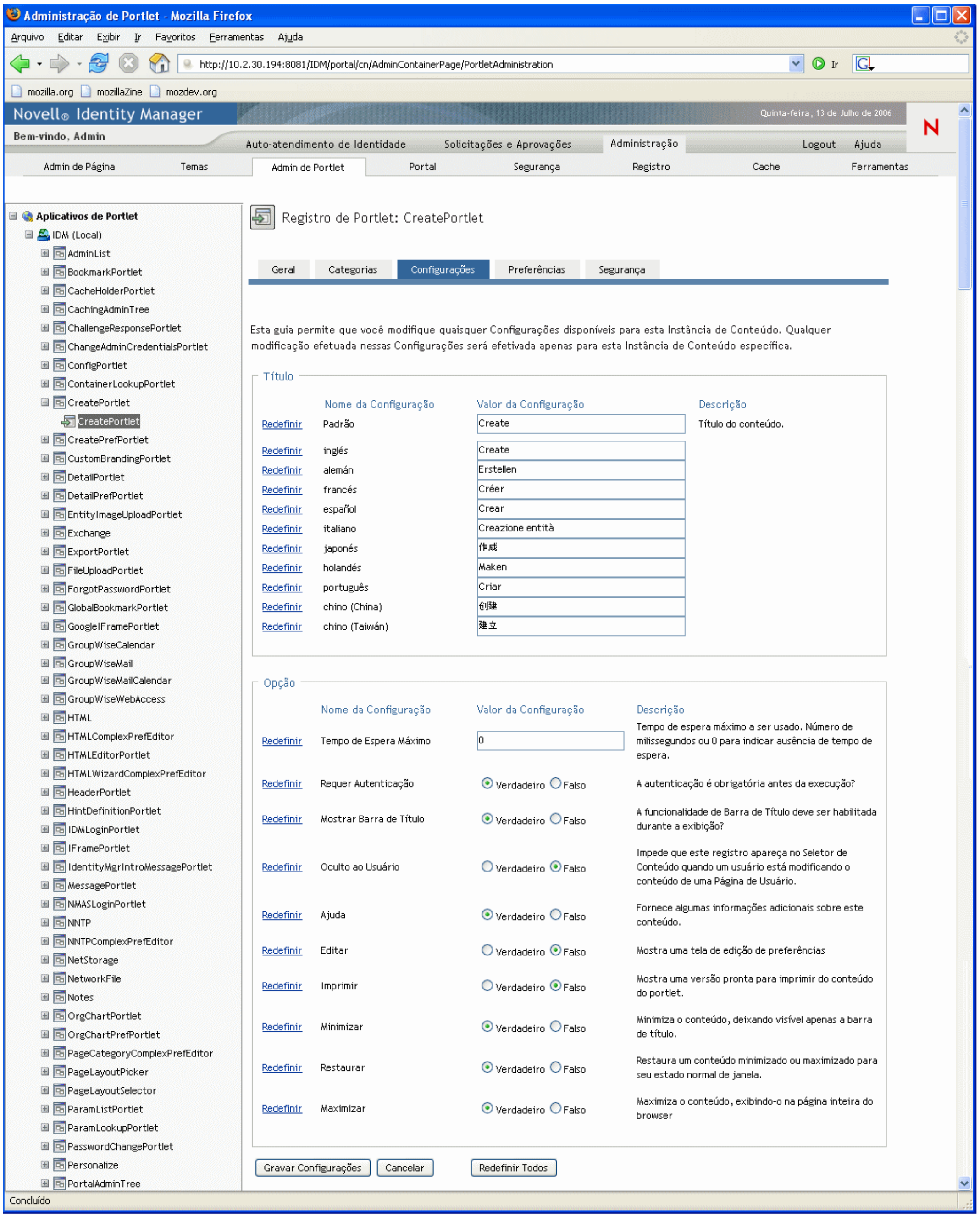
As configurações do Java Portlet 1.0 padrão são definidas no descritor de distribuição (portlet.xml) do WAR do aplicativo de portlet. Você pode mudar os valores dessas configurações em cada registro usando a página Administração de Portlet. Nesse caso, os novos valores só são ativados para o registro de portlet selecionado.

Para modificar configurações de registros de portlet:

1. Na lista Aplicativos de Portlet, *selecione* o registro de portlet cujas configurações você deseja modificar.

   Um painel *Geral* é exibido à direita.
2. Vá até o painel *Configurações*.

Esse painel exibe as configurações atuais para o registro de portlet selecionado:



3 *Modifique* as configurações conforme apropriado.

Lembre-se de que, nesse painel, você também pode executar as seguintes ações:

Se você deseja	Faça isto
Descartar mudanças que não foram gravadas	Clique em **Cancelar**

Se você deseja	Faça isto
Recuperar os valores padrão de todas as configurações do registro de portlet (como definido na definição de portlet correspondente)	Clique em **Redefinir Tudo**
Recuperar o valor padrão de uma configuração específica	Clique no link **Redefinir** ao lado da configuração

4 Clique em *Gravar Configurações*.

9.4.5 Modificando preferências de registros de portlet

As preferências do portlet são definidas pelo desenvolvedor no momento da criação no descritor de distribuição de portlet. As preferências variam de um portlet para outro de acordo com a implementação do desenvolvedor.

Você pode mudar os valores dessas preferências em cada registro usando a página Administração de Portlet. Nesse caso, os novos valores só são ativados para o registro de portlet selecionado.

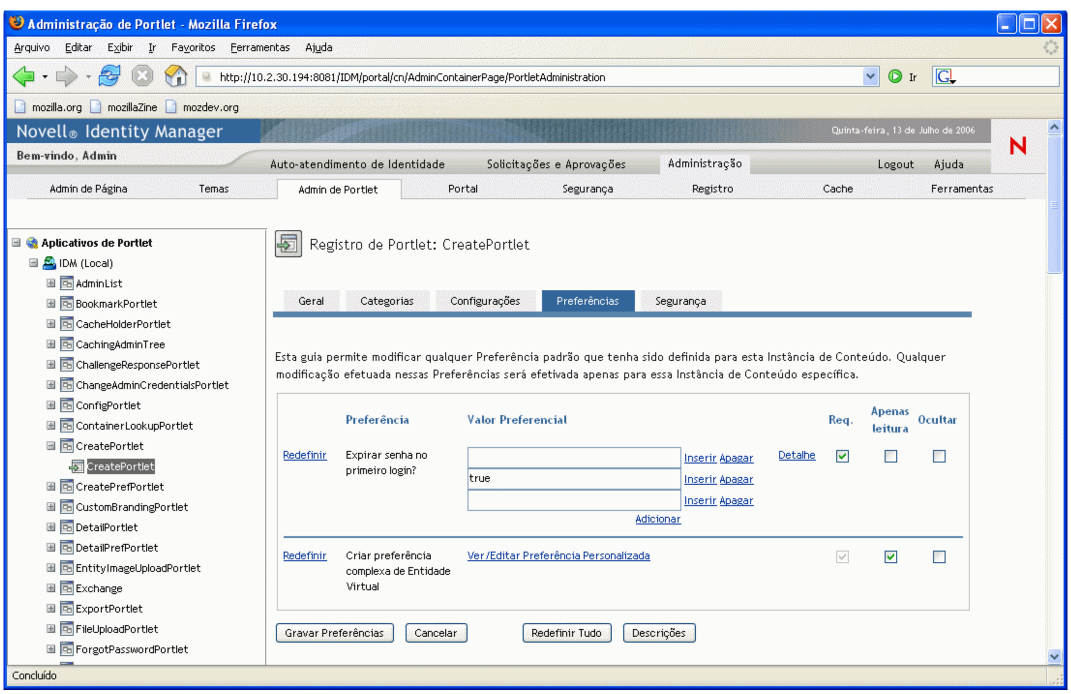
Para modificar preferências de registros de portlet:

1 Na lista Aplicativos de Portlet, *selecione* o registro de portlet cujas preferências você deseja modificar.

Um painel *Geral* é exibido à direita.

2 Vá até o painel *Preferências*.

Esse painel exibe as preferências atuais para o registro de portlet selecionado:



3 *Modifique* as preferências conforme apropriado.

Lembre-se de que, nesse painel, você também pode executar as seguintes ações:

Se você deseja	Faça isto
Exibir mais informações sobre as preferências	Clique em **Descrições**
Descartar mudanças que não foram gravadas	Clique em **Cancelar**
Recuperar os valores padrão de todas as preferências do registro de portlet (como estabelecido na definição de portlet correspondente)	Clique em **Redefinir Tudo**
Recuperar o valor padrão de uma preferência específica	Clique no link **Redefinir** ao lado da preferência

4 Para modificar a *versão localizada* de uma preferência para cada local especificado na definição de portlet, siga estas etapas:

4a Clique no link *Detalhe* ao lado da preferência (se disponível).

O painel exibe os valores de preferência de cada local.

4b *Modifique* os valores conforme apropriado.

4c Clique em *OK* para aplicar suas mudanças e retornar à principal lista de preferências.

5 Clique em *Gravar Preferências*.

9.4.6 Atribuindo permissões de segurança a registros de portlet

Você pode atribuir as seguintes permissões de segurança a usuários, grupos e containers para os registros de portlet:

Permissão	Descrição
Lista	Os usuários podem **ver** o registro de portlet em uma lista de seleções
Executar	Os usuários podem **executar** o registro de portlet em uma página do portal

Quando você modifica as permissões de segurança, os novos valores só são ativados para o registro de portlet selecionado.

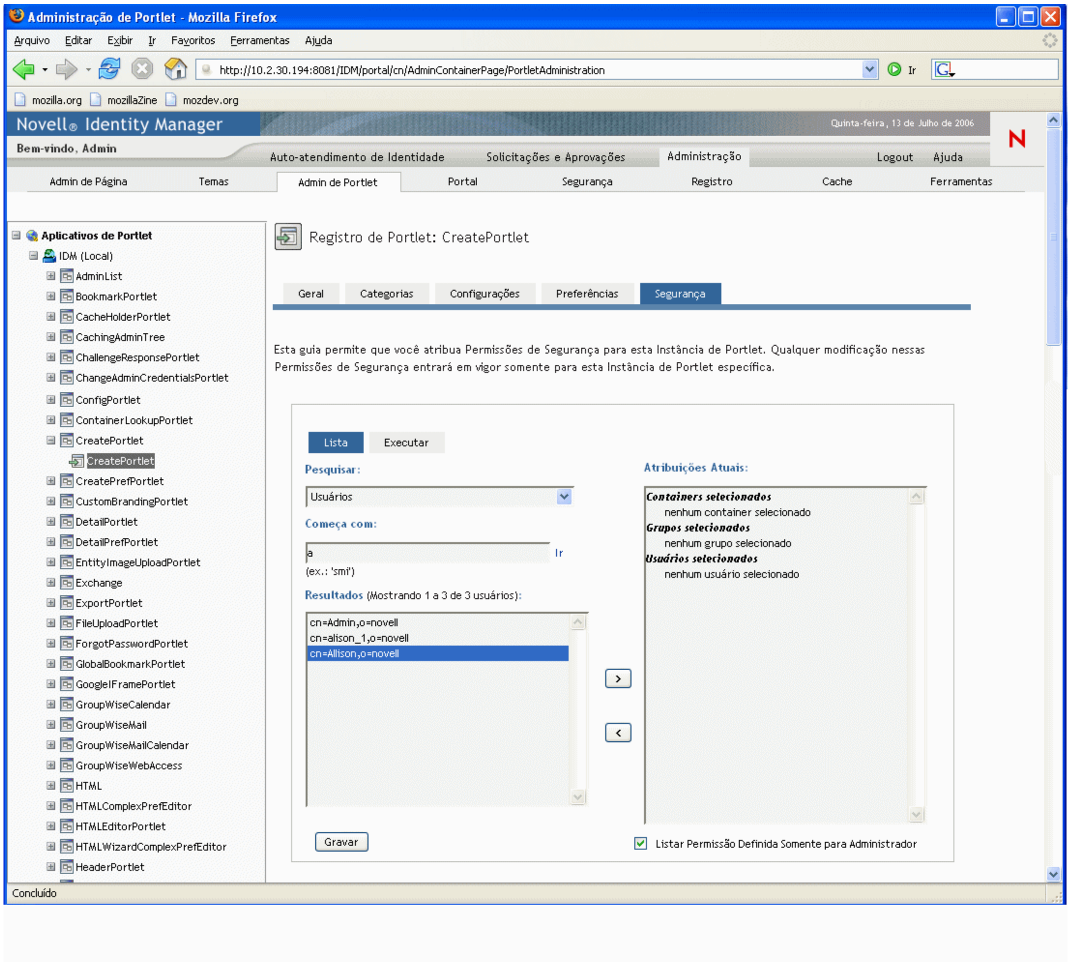
Para atribuir permissões de segurança a registros de portlet:

1 Na lista Aplicativos de Portlet, *selecione* o registro de portlet cujas permissões de segurança você deseja modificar.

Um painel *Geral* é exibido à direita.

2 Vá até o painel *Segurança*.

Esse painel exibe as permissões de segurança atuais para o registro de portlet selecionado:



3 Vá até a guia *Lista* ou *Executar*, dependendo do tipo de permissão a ser atribuído.

4 Especifique valores para as seguintes *configurações de pesquisa*:

Configuração	O que fazer
Pesquisar	Selecione uma das seguintes opções no menu suspenso: ◆ Usuários ◆ Grupos ◆ Containers

Configuração	O que fazer

Começa com	Se você deseja:
	◆ **Localizar todos** os objetos disponíveis do tipo que você especificou (usuário, grupo ou container), deixe esta configuração em branco.
	◆ **Localizar um subconjunto** desses objetos, informe os caracteres iniciais dos valores CN desejados. (Não há distinção entre maiúsculas e minúsculas, nem suporte a curingas.)
	Por exemplo, a busca por grupos que começam com `S` limita os resultados da pesquisa a algo como:
	`cn=Sales,ou=groups,o=MyOrg`
	`cn=Service,ou=groups,o=MyOrg`
	`cn=Shipping,ou=groups,o=MyOrg`
	Uma busca por grupos que começam com `Se` retorna:
	`cn=Service,ou=groups,o=MyOrg`

5 Clique em *Ir*.

Os resultados da pesquisa aparecem na lista *Resultados*.

6 *Selecione* os usuários, os grupos ou os containers que devem ser atribuídos ao registro de portlet e clique no botão *Adicionar* (>).

Dica: Mantenha a tecla *Control* pressionada para fazer várias seleções.

7 Habilite ou desabilite o recurso de *bloqueio* para o registro de portlet da seguinte maneira:

Se você deseja	Faça isto
Bloquear o registro de portlet de forma que somente o Administrador de Aplicativo de Usuário possa executá-lo	Marque **Listar/Executar Permissão Definida Somente para Administrador**
Permitir que todos os usuários, grupos e containers listem/executem o registro de portlet	Desmarque **Listar/Executar Permissão Definida Somente para Administrador** **Observação:** Se você desmarcar esta configuração mas não houver usuários, grupos ou containers explicitamente atribuídos ao registro de portlet, **todos terão permissão de Listar/Executar** para o registro de portlet.

8 Clique em *Gravar*.

9.4.7 Anulando o registro de um portlet

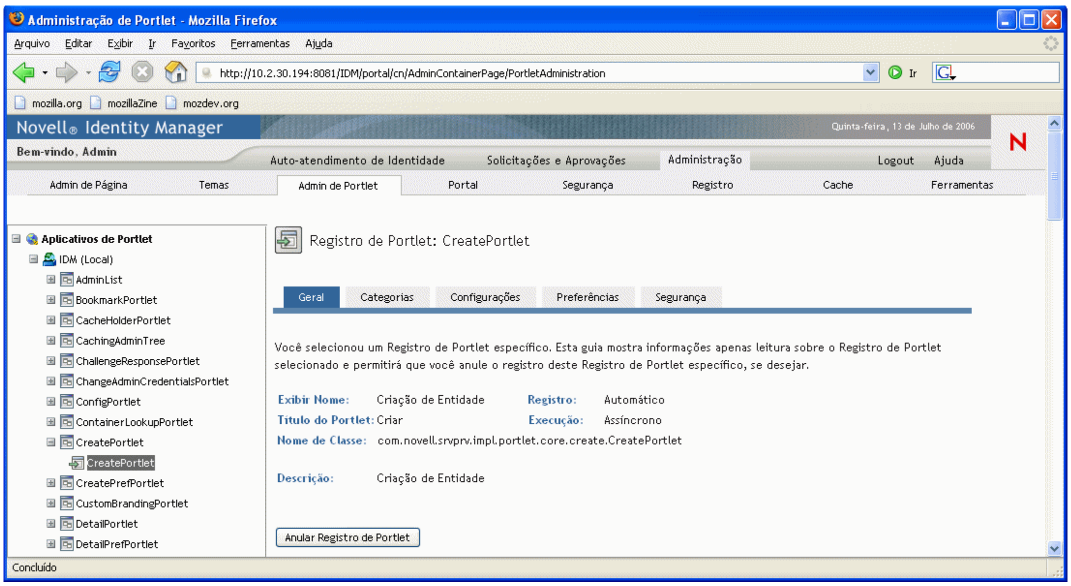
Você pode usar a página Administração de Portlet para anular o portlet se necessário.

Observação: Se você anular o registro de um portlet que esteja definido como *registrado automaticamente*, esse portlet será registrado mais uma vez automaticamente quando você reiniciar o servidor de aplicativos.

Para anular o registro de um portlet:

1 Na lista Aplicativos de Portlet, *selecione* o registro de portlet que você deseja anular.

É exibido um painel *Geral* à direita, com informações sobre o registro de portlet selecionado:



2 Clique em *Anular Registro de Portlet*.

3 Ao ser solicitado para confirmar a operação de anulação, clique em *OK*.

Configuração do portal

10

Este capítulo ensina a usar a página *Portal* da *guia Administração* da interface de usuário do Identity Manager. Os tópicos incluem:

Para obter informações gerais sobre como acessar e trabalhar com a guia Administração, consulte o Capítulo 6, "Usando a guia Administração" na página 131.

10.1 Sobre a configuração do portal

Você pode usar a página Portal para controlar as *características de portal* do aplicativo de usuário do Identity Manager e especificar como o aplicativo de usuário se conecta ao *cofre de identidade* (provedor do LDAP).

10.2 Configurações gerais

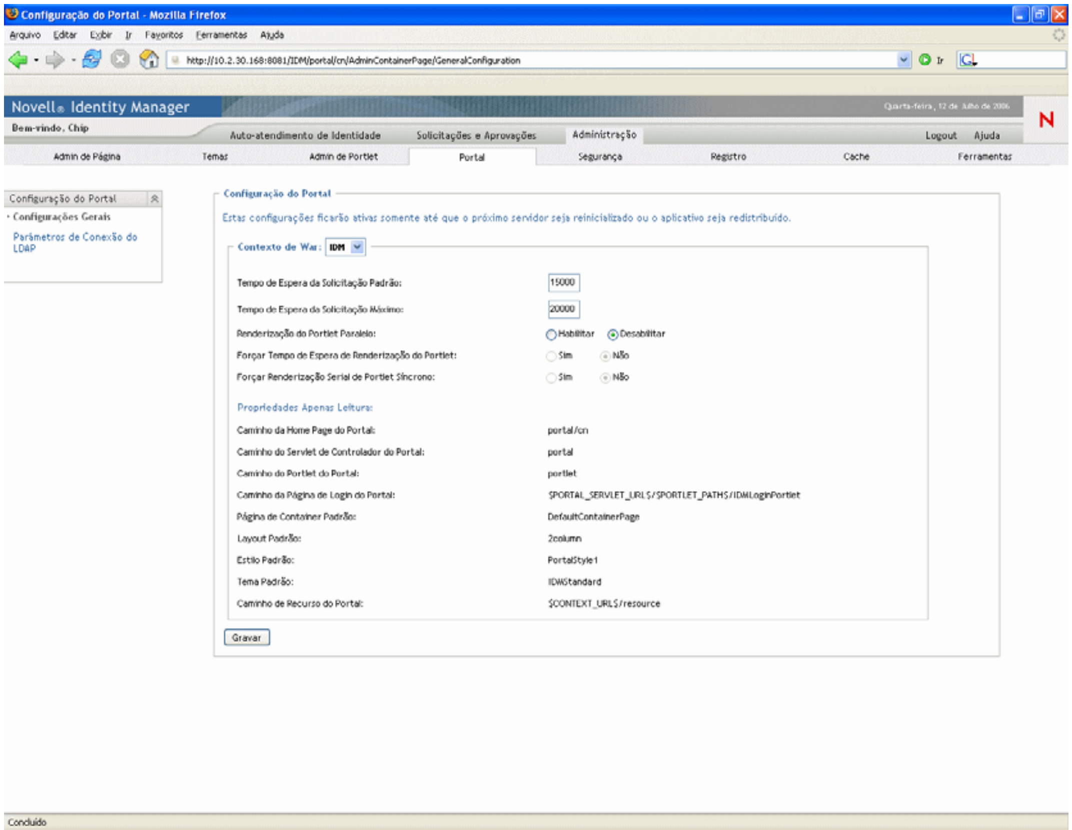
A página Portal contém um painel Configurações Gerais que pode ser usado para:

- *Mudar algumas características de portal* do aplicativo de usuário do Identity Manager temporariamente (até o aplicativo-servidor reiniciar novamente ou o usuário-aplicativo ser redistribuído novamente)
- *Ver outras características do portal* do aplicativo de usuário do Identity Manager

Para administrar configurações gerais:

1 Na página Portal, selecione *Configurações Gerais* no menu de navegação à esquerda.

O painel Configurações Gerais é exibido:



2 Se você tem mais de um *Contexto de War*, selecione aquele cujas configurações serão acessadas.

O painel é atualizado para mostrar as configurações atuais do contexto escolhido.

3 *Examine* e *Modifique* as configurações conforme apropriado. Para obter detalhes, consulte:

- Seção 10.2.1, “Configurações que podem ser mudadas” na página 200
- Seção 10.2.2, “Configurações apenas leitura” na página 202

4 Se você efetuar mudanças que queira aplicar, clique em *Gravar*.

10.2.1 Configurações que podem ser mudadas

Você pode modificar diversas configurações de portal no painel Configurações Gerais. Seus valores permanecem ativados até o aplicativo-servidor reiniciar novamente ou o usuário-aplicativo ser redistribuído novamente. Quando ocorrer um reinício ou uma redistribuição, essas configurações voltam a assumir os valores padrão do WAR do aplicativo de usuário.

Configuração	O que fazer
Tempo de Espera de Solicitação Padrão	Especifique o tempo padrão (em milissegundos) que uma solicitação aguarda antes de entrar em tempo de espera. Se nenhum portlet assíncrono definir um tempo de espera ou se nenhum portlet definir um tempo de espera que ultrapasse esse valor, o valor padrão será usado. Se um ou mais portlets a ser renderizado definir um tempo de espera superior ao valor padrão, será usado o valor maior em vez do padrão. Esta configuração pode ser usada para impedir que o aplicativo receba um excesso de mensagens sobre tempo de espera dos portlets (isso pode ocorrer se os portlets definirem valores muito baixos). **Observação:** Caso todos os portlets possam ser renderizados antes do tempo de espera padrão, a solicitação retornará ao cliente imediatamente.
Tempo de Espera de Solicitação Máximo	Especifique o tempo máximo (em milissegundos) que uma solicitação poderá esperar para ser concluída. Após esse tempo, toda solicitação retornará ao cliente, independentemente de algum portlet definir um valor de tempo de espera superior. Esta configuração pode ser usada para garantir que o portal responda em tempo, mesmo que um ou mais portlets definam um valor maior.
Renderização do Portlet Paralelo	Habilitar ou desabilitar a renderização assíncrona do portlet no portal. Este é um recurso avançado que é desabilitado por padrão. Se você habilitar o recurso, o portal atribuirá solicitações de renderização assíncronas a threads individuais (o que permite aos portlets renderizar conteúdo em paralelo). Quando esse recurso é desabilitado, todos os portlets renderizam conteúdo sincronamente no principal thread da solicitação.
Forçar Tempo de Espera de Renderização do Portlet	Determine se os portlets assíncronos serão delegados ao principal thread da solicitação para renderizar conteúdo se não houver threads disponíveis no pool de threads. Se você escolher **Não**, os portlets assíncronos poderão ser executados no principal thread da solicitação se não houver threads individuais disponíveis. Se você escolher **Sim**, os portlets assíncronos serão forçados a aguardar que haja thread individuais disponíveis para que eles possam processar conteúdo. Se ocorrer tempo de espera antes que os portlets executem a solicitação de renderização, será gerada uma mensagem de erro específica na janela do portlet.

Configuração	O que fazer
Forçar Renderização Serial de Portlet Síncrono	Determinar como os portlets síncronos são executados. Se você escolher **Sim**, todos os portlets síncronos serão executados no principal thread da solicitação. Se você escolher **Não**, o portal poderá alocar um thread separado para processar solicitações de renderização síncronas (o que evita gargalos no principal thread da solicitação).

10.2.2 Configurações apenas leitura

As seguintes configurações são exibidas apenas para fins informativos e não podem ser mudadas no painel Configurações Gerais:

Caminho da Home Page do Portal	Layout Padrão
Caminho do Servlet de Controlador do Portal	Estilo Padrão
Caminho do Portlet do Portal	Tema Padrão
Caminho da Página de Login do Portal	Caminho de Recurso do Portal
Página de Container Padrão	

Os valores dessas configurações são definidos no WAR do aplicativo de usuário. (Lembre-se de que o Tema Padrão reflete sua atual opção de tema na página Temas.)

10.3 Parâmetros de Conexão LDAP

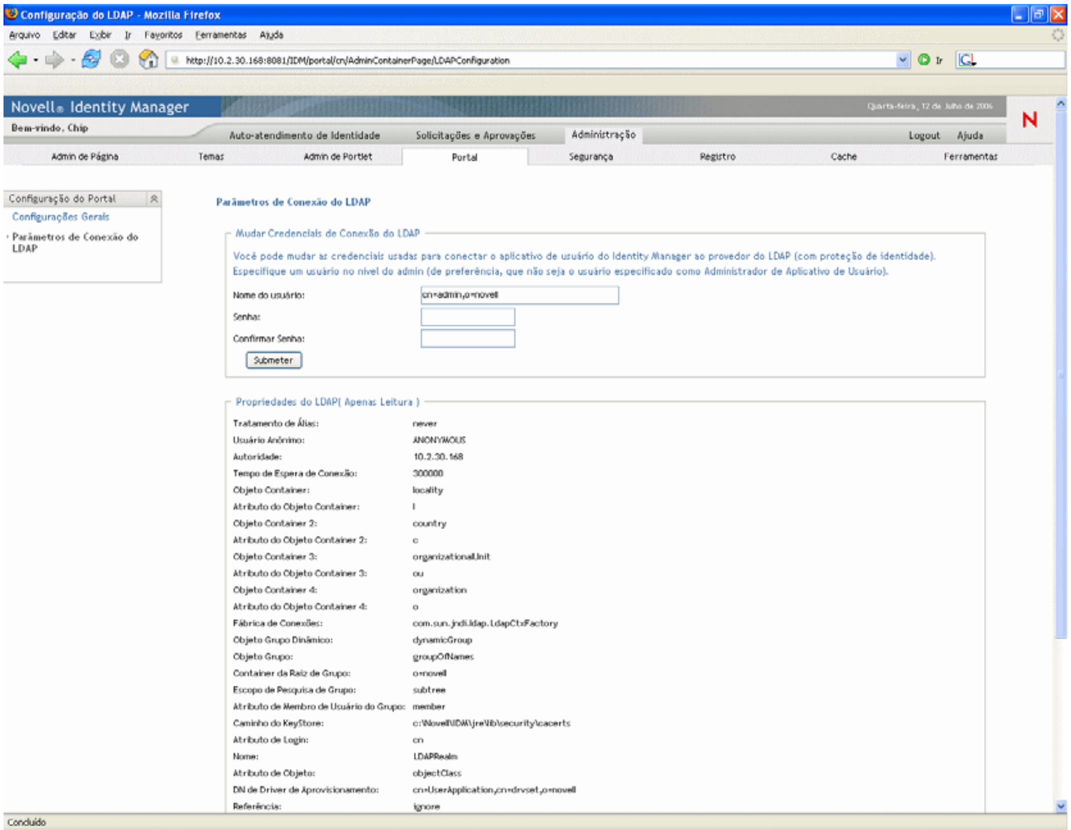
A página Portal contém um painel Parâmetros de Conexão LDAP que pode ser usado para:

- *Mudar as credenciais* usadas pelo aplicativo de usuário do Identity Manager durante a conexão com o cofre de identidade (provedor LDAP)
- *Ver outras propriedades LDAP* do aplicativo de usuário do Identity Manager

Para administrar os parâmetros de conexão LDAP:

1 Na página Portal, selecione *Parâmetros de Conexão LDAP* no menu de navegação à esquerda.

O painel Parâmetros de Conexão LDAP é exibido:



2 *Examine* e *Modifique* as configurações conforme apropriado. Para obter detalhes, consulte:

- Seção 10.2.1, “Configurações que podem ser mudadas” na página 200
- Seção 10.3.2, “Configurações apenas leitura” na página 204

3 Se você efetuar mudanças que queira aplicar, clique em *Submeter*.

10.3.1 Configurações que podem ser mudadas

No painel Parâmetros de Conexão LDAP, você pode modificar as configurações das credenciais a serem usadas pelo aplicativo de usuário do Identity Manager sempre que ele se conectar ao cofre de identidade (provedor LDAP). As mudanças efetuadas nesse painel serão gravadas no banco de dados do aplicativo de usuário para serem usadas em tempo de execução, e serão verificadas no cofre de identidade. (Esse painel não atualiza os valores de credenciais originais registrados no WAR do aplicativo de usuário durante a instalação.)

Configuração	O que fazer
Nome do usuário	Digite o nome de um usuário que tenha direitos totais de **administrador** no cofre de identidade. O aplicativo de usuário do Identity Manager precisa ter acesso ao cofre de identidade como um administrador para funcionar. É comum especificar o administrador da **raiz** do cofre de identidade como o nome de usuário da conexão LDAP. O administrador da raiz tem controle total sobre a árvore. Portanto, não é preciso designar direitos de trustee especiais. Por exemplo: `cn=admin,o=myorg` Se você especificar algum outro usuário, precisará designar direitos de trustee que podem ser herdados às propriedades [Direitos a Todos os Atributos] e [Direitos de Entrada] do Driver de Aplicativo do Usuário. **Observação:** Para evitar confusão, é recomendável **não** especificar o Administrador como o nome de usuário da conexão LDAP. É melhor usar contas separadas para esses dois tipos de finalidade.
Senha e Confirmar Senha	Digite a senha definida para esse nome de usuário no cofre de identidade.

10.3.2 Configurações apenas leitura

As seguintes configurações são exibidas apenas para fins informativos e não podem ser mudadas no painel Parâmetros da Conexão LDAP:

ALIAS_HANDLING	GROUP_USER_MEMBER_ATTRIB
ANONYMOUS_USER	KEYSTORE_PATH
AUTHORITY	LOGIN_ATTRIBUTE
CONNECTION_TIMEOUT	NAME
CONTAINER_OBJECT	OBJECT_ATTRIB
CONTAINER_OBJECT_ATTRIB	PROVISION_ROOT
CONTAINER_OBJECT2	REFERRAL
CONTAINER_OBJECT2_ATTRIB	ROOT_NAME
CONTAINER_OBJECT3	USE_DYNAMIC_GROUPS
CONTAINER_OBJECT3_ATTRIB	USE_REGISTERED_DYNAMIC_GROUPS
CONTAINER_OBJECT4	USE_SSL

CONTAINER_OBJECT4_ATTRIB	USER_GROUP_MEMBER_ATTRIB
CONTEXT_FACTORY	USER_OBJECT
DYNAMIC_GROUP_OBJECT	USER_ROOT_CONTAINER
GROUP_OBJECT	USER_SEARCH_SCOPE
GROUP_ROOT_CONTAINER	UUID_ATTRIB
GROUP_SEARCH_SCOPE	UUID_AUX_CLASS

Os valores dessas configurações são determinados quando você instala o aplicativo de usuário.

11 Configuração de segurança

Este capítulo informa como usar a página *Segurança* da guia *Administração* da interface de usuário do Identity Manager. Os tópicos incluem:

- Seção 11.1, “Sobre a configuração de segurança” na página 207
- Seção 11.2, “Designando o Administrador de Aplicativo de Usuário” na página 208

Para obter informações gerais sobre como acessar e trabalhar com a guia Administração, consulte o Capítulo 6, “Usando a guia Administração” na página 131.

11.1 Sobre a configuração de segurança

Você pode usar a página Segurança para especificar quem será *Administrador* do aplicativo de usuário do Identity Manager.

Um Administrador de Aplicativo de Usuário tem autorização para realizar todas as funções de gerenciamento relacionadas ao aplicativo de usuário do Identity Manager. Uma dessas funções é acessar a guia Administração da interface de usuário do Identity Manager para executar ações administrativas.

Durante a instalação, um usuário é especificado como o Administrador de Aplicativo de Usuário. Após a instalação, esse usuário pode utilizar a página Segurança para especificar outros Administradores de Aplicativo de Usuário, conforme necessário.

Normalmente, o usuário que será Administrador de Aplicativo de Usuário deve estar *localizado no container da raiz do usuário* especificado na configuração LDAP do aplicativo de usuário. Dessa forma, ele pode efetuar login apenas com o nome de usuário (em vez de precisar do nome exclusivo a cada vez). Também é comum esse usuário ter *direitos de manter e criar objetos* na árvore, embora isso não seja obrigatório.

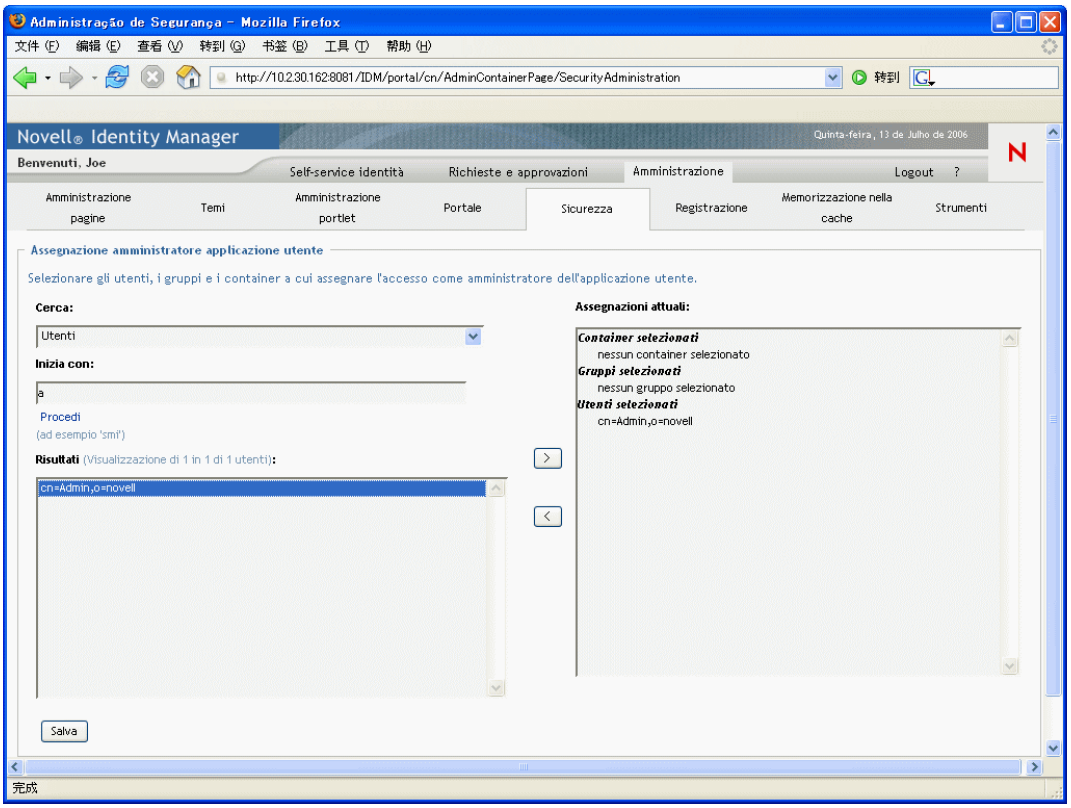
Observação: Se necessário, um Administrador de Aplicativo de Usuário pode permitir que um ou mais usuários vejam e acessem páginas específicas da guia Administração. Essas permissões são atribuídas com a página *Admin de Página* da guia Administração. (Para obter detalhes, consulte o Capítulo 7, “Administração de Página” na página 137.)

11.2 Designando o Administrador de Aplicativo de Usuário

Ao designar Administradores de Aplicativo de Usuário, você poderá especificar usuários, grupos ou containers.

Para designar Administradores de Aplicativo de Usuário:

1 Vá até a página *Segurança*:



2 Especifique valores para as seguintes *configurações de pesquisa*:

Configuração	O que fazer
Pesquisar	Selecione uma das seguintes opções no menu suspenso: ◆ Usuários ◆ Grupos ◆ Containers

Configuração	O que fazer

Começa com	Se você deseja:
	◆ **Localizar todos** os objetos disponíveis do tipo que você especificou (usuário, grupo ou container), deixe esta configuração em branco.
	◆ **Localizar um subconjunto** desses objetos, informe os caracteres iniciais dos valores CN desejados. (Não há distinção entre maiúsculas e minúsculas, nem suporte a curingas.)
	Por exemplo, a busca por grupos que começam com `S` limita os resultados da pesquisa a algo como:
	`cn=Sales,ou=groups,o=MyOrg`
	`cn=Service,ou=groups,o=MyOrg`
	`cn=Shipping,ou=groups,o=MyOrg`
	Uma busca por grupos que começam com `Se` retorna:
	`cn=Service,ou=groups,o=MyOrg`

3 Clique em *Ir*.

Os resultados da pesquisa aparecem na lista *Resultados*.

4 *Selecione* os usuários, os grupos ou os containers que devem ser atribuídos como Administradores de Aplicativo de Usuário e clique no botão *Adicionar* (>).

Dica: Mantenha a tecla *Control* pressionada para fazer várias seleções.

5 Clique em *Gravar*.

Para desatribuir Administradores de Aplicativo de Usuário:

1 Na lista *Atribuições Atuais*, selecione os usuários, os grupos ou os containers cuja atribuição como Administradores de Aplicativo de Usuário deve ser removida e clique no botão *Remover* (<).

Dica: Mantenha a tecla *Control* pressionada para fazer várias seleções.

2 Clique em *Gravar*.

Configuração de Registro 12

Este capítulo informa como usar a página *Registro* da guia *Administração* da interface de usuário do Identity Manager. Os tópicos incluem:

Para obter informações gerais sobre como acessar e trabalhar com a guia Administração, consulte o Capítulo 6, "Usando a guia Administração" na página 131.

12.1 Sobre a configuração de registro

Você pode usar a página Registro para controlar os *níveis de mensagens de registro* que o aplicativo de usuário do Identity Manager deve gerar, e especificar se essas mensagens serão enviadas ao *Novell Audit*.

O aplicativo de usuário do Identity Manager implementa o recurso de registro usando o *log4j*, um pacote de registro de código-fonte aberto distribuído pela Apache Software Foundation. Por padrão, as mensagens de evento são registradas nestes dois locais:

- *O console do sistema* do servidor de aplicativos onde o aplicativo de usuário do Identity Manager foi distribuído
- *Um arquivo de registro* nesse servidor de aplicativos, por exemplo:

```
jboss/server/IDM/log/server.log
```

Esse é um arquivo de registro transferível. Ao alcançar determinado tamanho, ele passa para outro arquivo, e assim sucessivamente.

Caso tenha configurado seu ambiente para incluir o Novell Audit, você também tem a opção de registrar mensagens de evento.

Para obter detalhes sobre como configurar seu ambiente de registro e o Novell Audit, consulte o Capítulo 5, "Configurando o registro" na página 119.

12.2 Sobre os registros

A página Registro contém uma variedade de registros, cada qual com mensagens de evento de uma parte diferente do aplicativo de usuário do Identity Manager. Cada registro tem seu próprio nível de saída independente.

Os nomes de registro baseiam-se em convenções do log4j. Você verá esses nomes de registro nas mensagens de evento geradas, o que indica o contexto da saída da mensagem.

Nome do registro	Descrição
com.novell	Pai de outros registros do aplicativo de usuário do Identity Manager
com.novell.afw.portal.aggregation	Mensagens relacionadas ao processamento de páginas do portal
com.novell.afw.portal.persist	Mensagens relacionadas à persistência dos dados do portal (incluindo páginas do portal e registros do portlet)
com.novell.afw.portal.portlet	Mensagens dos portlets principais do portal e dos portlets acessórios
com.novell.afw.portal.util	Mensagens dos portlets de importação, exportação e navegação
com.novell.afw.portlet.consumer	Mensagens relacionadas à renderização do portlet
com.novell.afw.portlet.core	Mensagens relacionadas à API do portlet principal
com.novell.afw.portlet.persist	Mensagens relacionadas à persistência dos dados do portlet (incluindo valores de preferências e configurações do portlet)
com.novell.afw.portlet.producer	Mensagens relacionadas ao registro e à configuração de portlets no portal
com.novell.afw.portlet.util	Mensagens relacionadas ao código de utilitário usado pelos portlets
com.novell.afw.theme	Mensagens do subsistema de temas
com.novell.afw.util	Mensagens relacionadas a classes de utilitário do portal
com.novell.soa.af.impl	Mensagens do subsistema do fluxo de aprovações (workflow de aprovisionamento)
com.novell.srvprv.apwa	Mensagens do aplicativo Web Solicitações e Aprovações (ações e tags)
com.novell.srvprv.impl.portlet.core	Mensagens dos principais portlets de identidade e portlets de senha
com.novell.srvprv.impl.portlet.util	Mensagens dos portlets de utilitário relacionados a identidade
com.novell.srvprv.impl.servlet	Mensagens dos serviços ajax e servlet ajax da estrutura de controle de IU
com.novell.srvprv.impl.uictrl	Mensagens da API do Registro de controle de IU e renderização do formulário de aprovação
com.novell.srvprv.impl.vdata	Mensagens da camada de abstração do diretório
com.novell.srvprv.spi	Mensagens da API do Registro de controle de IU
com.sssw.fw.cachemgr	Mensagens relacionadas ao subsistema de cache de estrutura
com.sssw.fw.core	Mensagens relacionadas ao subsistema principal de estrutura

Nome do registro	Descrição
com.sssw.fw.directory	Mensagens relacionadas ao subsistema de diretórios de estrutura
com.sssw.fw.event	Mensagens relacionadas ao subsistema de eventos de estrutura
com.sssw.fw.factory	Mensagens relacionadas ao subsistema de fábrica de estrutura
com.sssw.fw.persist	Mensagens relacionadas ao subsistema de persistência de estrutura
com.sssw.fw.resource	Mensagens relacionadas ao subsistema de recursos de estrutura
com.sssw.fw.security	Mensagens relacionadas ao subsistema de segurança de estrutura
com.sssw.fw.server	Mensagens relacionadas ao subsistema de servidores de estrutura
com.sssw.fw.servlet	Mensagens relacionadas ao subsistema de servlets de estrutura
com.sssw.fw.session	Mensagens relacionadas ao subsistema de sessões de estrutura
com.sssw.fw.usermgr	Mensagens relacionadas ao subsistema de usuários de estrutura
com.sssw.fw.util	Mensagens relacionadas ao subsistema de utilitários de estrutura
com.sssw.portal.manager	Mensagens relacionadas ao Portal Manager
com.sssw.portal.persist	Mensagens relacionadas à persistência do portal

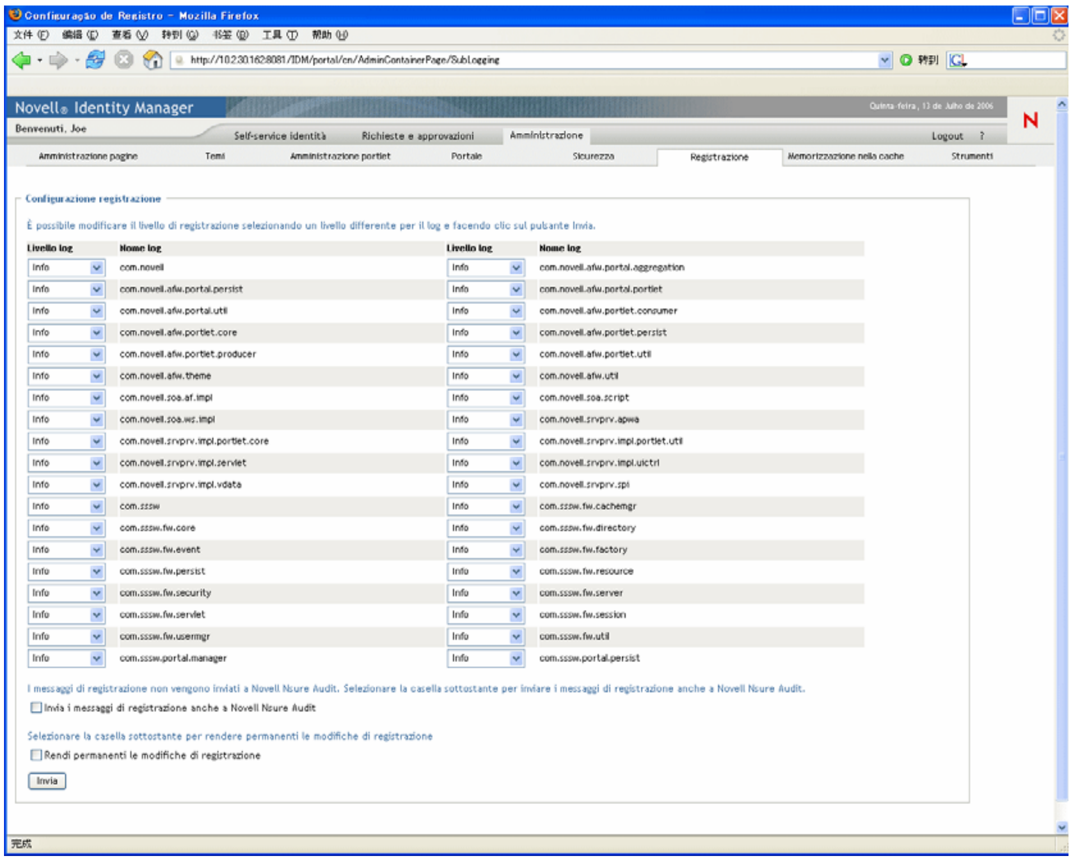
Lembre-se de que os registros do aplicativo de usuário são hierárquicos. Por exemplo, com.novell é o registro pai dos outros a ele subordinados. Os registros adicionais herdarão suas propriedades.

12.3 Mudando níveis de registro

Para controlar o volume de informações gravadas em determinado registro, mude o nível definido para ele. Por padrão, todos os registros são definidos como *Informações*, que é um nível intermediário.

Para mudar níveis de registro:

1 Vá até a página *Registro*:



2 Na parte superior da página, *procure um registro* cujo nível você queira mudar.

3 Use o menu suspenso para *selecionar* um dos seguintes níveis:

Nível	Descrição
Fatal	**O menos detalhado:**
	Grava erros fatais no registro
Erro	Grava erros (e tudo acima) no registro
Avisar	Grava avisos (e tudo acima) no registro
Informações	Grava mensagens informativas (e tudo acima) no registro
Depurar	Grava mensagens de depuração (e tudo acima) no registro

Nível	Descrição
Rastreamento	**O mais detalhado:** Grava informações de rastreamento (e tudo acima) no registro

4 *Repita a* Etapa 2 e a Etapa 3 para outros registros se necessário.

5 Clique em *Submeter*.

12.4 Enviando mensagens de registro para o Novell Audit

Você pode usar a página Registro para controlar se o aplicativo de usuário do Identity Manager envia saídas de mensagens de evento ao Novell Audit. Por padrão, o registro do Novell Audit fica desativado, a não ser que você o ative ao instalar o aplicativo de usuário.

Para ativar e desativar o registro no Novell Audit

1 Vá até a página *Registro*.

2 *Marque ou desmarque* a seguinte configuração conforme apropriado:

```
Enviar também mensagens de registro para a Auditoria
```

3 Clique em *Submeter*.

12.5 Mantendo suas configurações de registro

Por padrão, as mudanças efetuadas na página Registro permanecem ativas até o aplicativo-servidor reiniciar novamente ou o usuário-aplicativo ser redistribuído. Depois disso, as configurações de registro retomam seus valores padrão.

A página Registro, entretanto, oferece a opção de manter as mudanças efetuadas nas configurações. Se você ativar esse recurso, os valores das configurações de registro serão armazenadas em um *arquivo de configuração de registro* no servidor de aplicativos onde o aplicativo de usuário do Identity Manager foi distribuído. Por exemplo:

```
jboss/server/IDM/conf/extendlogging.xml
```

Para ativar e desativar a persistência das configurações:

1 Vá até a página *Registro*.

2 *Marque ou desmarque* a seguinte configuração conforme apropriado:

```
Manter as mudanças no registro
```

3 Clique em *Submeter*.

Configuração de cache 13

Este capítulo informa como usar a página *Cache* da guia *Administração* da interface de usuário do Identity Manager. Os tópicos incluem:

Para obter informações gerais sobre como acessar e trabalhar com a guia Administração, consulte o Capítulo 6, "Usando a guia Administração" na página 131.

13.1 Sobre a configuração de cache

Você pode usar a página Cache para gerenciar vários *caches* mantidos pelo aplicativo de usuário do Identity Manager. O aplicativo de usuário usa esses caches para armazenar dados temporários reutilizáveis no servidor de aplicativos de forma a otimizar o desempenho.

Quando necessário, você pode controlar esses caches *descarregando seu conteúdo* e *mudando suas configurações*.

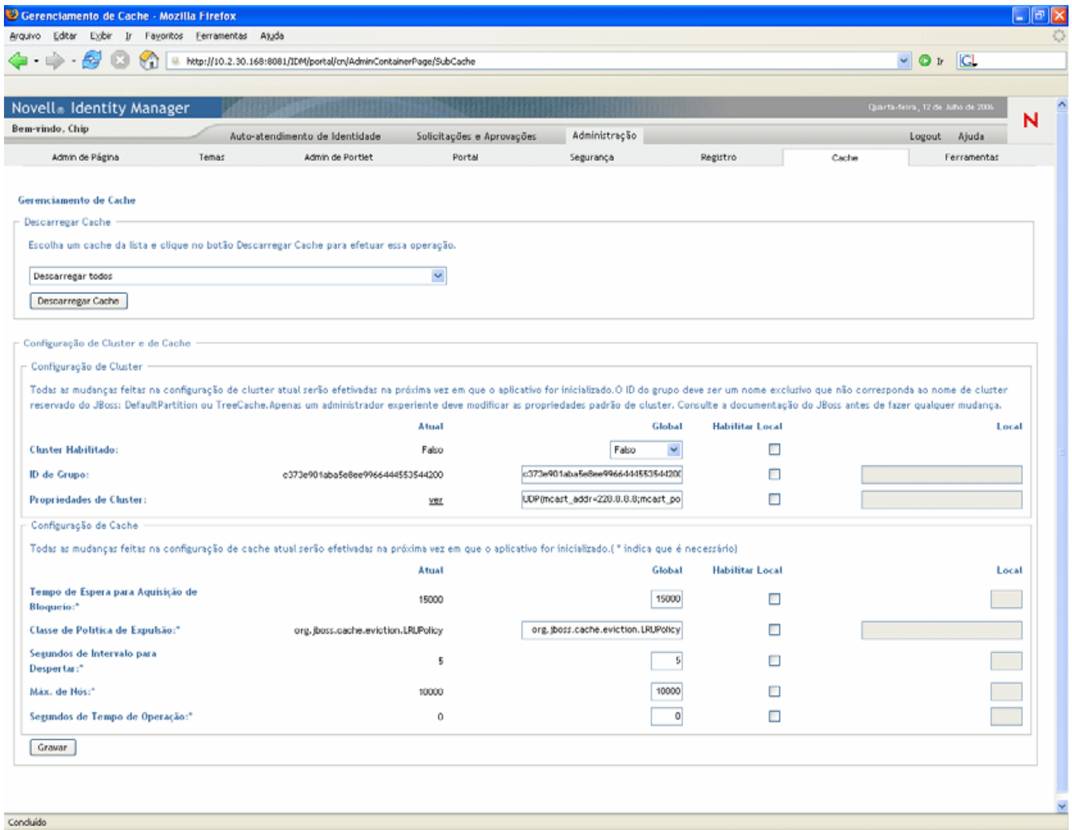
13.2 Descarregando caches

Os caches são nomeados de acordo com os *subsistemas* que os utilizam no aplicativo de usuário do Identity Manager. Normalmente, você não precisa descarregá-los, pois o aplicativo de usuário faz isso automaticamente com base na freqüência com que seus dados são usados ou quando os dados

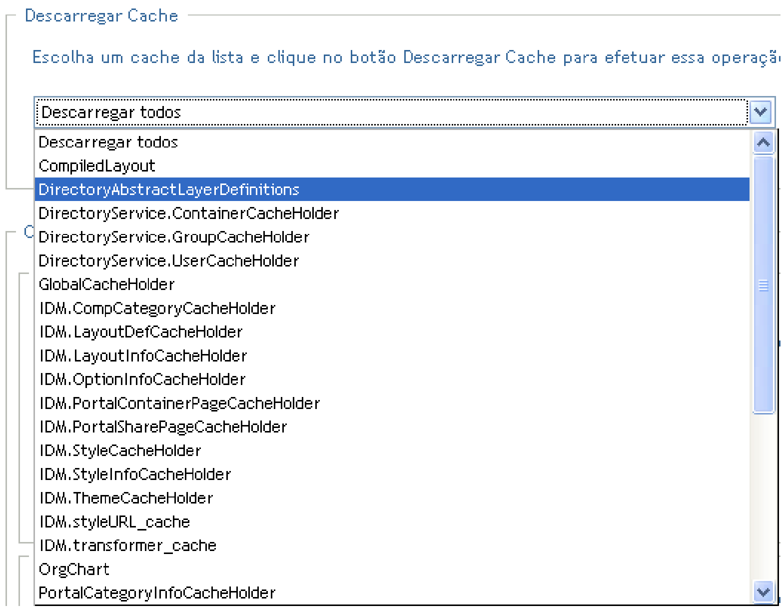
de origem sofrem alguma mudança. Contudo, se preciso, você pode *descarregar manualmente* caches selecionados ou todos os caches.

Para descarregar caches:

1 Vá até a página *Cache*:



2 Na seção *Descarregar Cache* da página, use o menu suspenso para *selecionar* determinado cache para ser descarregado (ou selecione *Descarregar todos*):



Lembre-se de que a lista de caches disponíveis é *dinâmica*; ela muda de acordo com os dados que estão armazenados em cache.

3 Clique no botão *Descarregar Cache*.

13.2.1 Descarregando o cache da camada de abstração do diretório

A *camada de abstração do diretório* do aplicativo de usuário também tem um cache. O cache *DirectoryAbstractLayerDefinitions* armazena definições da camada de abstração no servidor de aplicativos para otimizar o desempenho de todas as operações do modelo de dados.

Em uma situação típica, o aplicativo de usuário mantém automaticamente o cache DirectoryAbstractLayerDefinitions sincronizado com as definições da camada de abstração armazenadas no cofre de identidade. Entretanto, se necessário, é possível descarregar o cache DirectoryAbstractLayerDefinitions manualmente (como descrito acima) para forçar o carregamento das últimas definições do cofre de identidade.

Para obter mais informações sobre a camada de abstração do diretório do aplicativo de usuário, consulte o Capítulo 4, “Configurando a Camada de Abstração do Diretório” na página 75.

13.2.2 Descarregando caches em um cluster

A descarga de cache tem suporte em ambientes em cluster e sem cluster do servidor de aplicativos. Se o servidor de aplicativos integrar um cluster e você descarregar um cache manualmente, esse cache será *descarregado em todos os servidores* do cluster automaticamente.

13.3 Definindo configurações de cache

Você pode usar a página Cache para exibir e mudar as definições de configuração de cache de um ambiente de servidor de aplicativos *em cluster ou sem cluster*. Suas mudanças são gravadas imediatamente, mas só serão ativadas no próximo *reinício do usuário-aplicativo*.

Dica: Para reiniciar o aplicativo de usuário, você pode proceder de uma das seguintes maneiras: reinicializar o servidor de aplicativos, redistribuir o aplicativo (se WAR foi mudado de alguma forma) ou forçar o aplicativo a reiniciar (como descrito na documentação do seu servidor de aplicativos).

Para definir configurações de cache, considere o seguinte:

- Seção 13.3.1, "Como o cache é implementado" na página 220
- Seção 13.3.2, "Como as configurações de cache são armazenadas" na página 220
- Seção 13.3.3, "Como as configurações de cache são exibidas" na página 222
- Seção 13.3.4, "Configurações básicas de cache" na página 222
- Seção 13.3.5, "Configurações de cache para clusters" na página 224

13.3.1 Como o cache é implementado

No aplicativo de usuário do Identity Manager, o cache é implementado por meio do *JBoss Cache*. JBoss Cache é uma arquitetura de cache de código-fonte aberto que está incluída no JBoss Application Server, mas também é executada em outros servidores de aplicativos.

Para saber mais sobre a JBoss Cache, vá até www.jboss.org/products/jbosscache (http://www.jboss.org/products/jbosscache).

13.3.2 Como as configurações de cache são armazenadas

Existem *dois níveis de configurações* disponíveis para você controlar a configuração de cache. Você pode utilizá-los para ajustar o comportamento do cache do aplicativo de usuário do Identity Manager.

Nível	Descrição

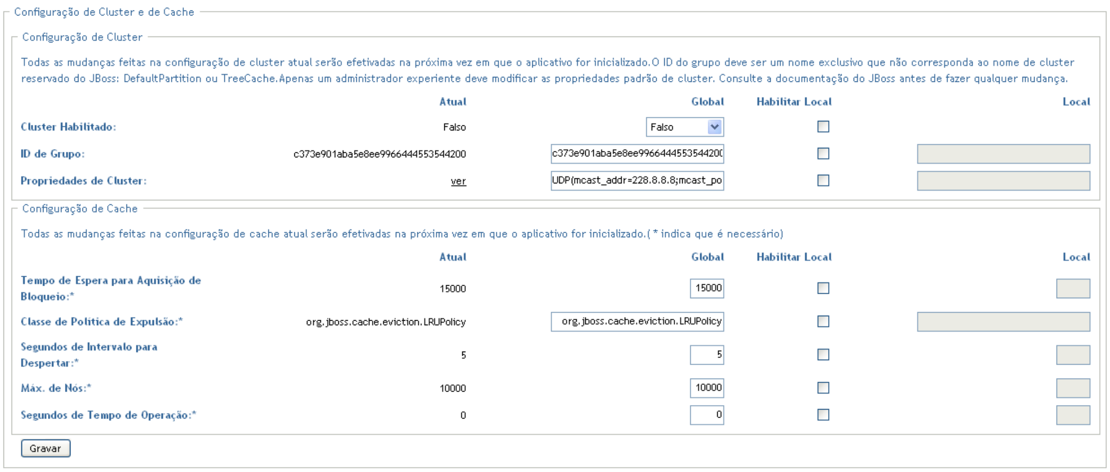
Configurações globais	As configurações globais estão **armazenadas em um local central** (o cofre de identidade) para que os diversos servidores de aplicativos possam usar os mesmos valores de configuração. Por exemplo, alguém que tenha um cluster de servidores de aplicativos normalmente usa configurações globais para os valores de configuração do cluster.
	
	Para **encontrar as configurações globais** no cofre de identidade, procure o seguinte objeto no driver do aplicativo de usuário do Identity Manager:
	
	`configuration.AppDefs.AppConfig`
	
	Por exemplo:
	
	`configuration.AppDefs.AppConfig.MyUserApplicationDriver.MyDriverSet.MyOrg`
	
	O **atributo XmlData** do objeto Configuração contém os dados de configurações globais.

Configurações locais	As configurações locais são **armazenadas separadamente em cada servidor de aplicativos** para que determinado servidor possa **anular** o valor de uma ou mais configurações globais. Por exemplo, convém especificar uma configuração local para remover um servidor de aplicativos do cluster especificado nas configurações globais ou talvez reatribuir um servidor a outro cluster.
	
	Para **encontrar as configurações locais** em seu servidor de aplicativos, procure este arquivo no diretório conf da configuração do servidor JBoss:
	
	`sys-configuration-xmldata.xml`
	
	Por exemplo:
	
	`jboss/server/IDM/conf/sys-configuration-xmldata.xml`
	
	Se seu servidor tem configurações locais, os dados estão contidos nesse arquivo. (Se não houver configurações locais especificadas, o arquivo não existe.)

Você deve considerar as configurações globais como os *valores padrão* de todo servidor de aplicativos que utiliza determinada instância do driver do aplicativo de usuário. Uma mudança em uma configuração global *afeta cada um desses servidores* (no próximo reinício de usuário-aplicativo), exceto nos casos em que um servidor específico estabelece um valor local que a anule.

13.3.3 Como as configurações de cache são exibidas

A página Cache exibe as *atuais configurações de cache* (desde o último reinício de usuário-aplicativo). Ela também exibe os *valores globais e locais* dessas configurações, e permite que você as *mude* (para usar no próximo reinício de usuário-aplicativo).



As configurações globais sempre têm valores. As configurações locais são opcionais.

13.3.4 Configurações básicas de cache

Essas configurações de cache se aplicam a servidores de aplicativos em cluster e sem cluster.

Para definir configurações básicas de cache:

1 Vá até a página *Cache*.

2 Na seção *Configuração de Cache* da página, especifique *valores globais ou locais* para as seguintes configurações, conforme apropriado:

Configuração	O que fazer
Tempo de Espera para Aquisição de Bloqueio	Especifique o **intervalo de tempo (em milissegundos)** que o cache aguarda por um bloqueio em um objeto. Você pode aumentar essa configuração se o aplicativo de usuário receber muitas exceções de tempo de espera de bloqueio no registro do aplicativo. O padrão é 15000 ms.

Configuração	O que fazer
Classe de Política de Expulsão	Especifique o **nome de classe** da política de expulsão de cache a ser usada. O padrão é a política de expulsão do LRU que o Jboss Cache oferece: `org.jboss.cache.eviction.LRUPolicy` Se apropriado, você poderá mudá-la para outra política que tenha o suporte do JBoss Cache. Para saber sobre as políticas de expulsão suportadas, vá até www.jboss.org/products/jbosscache (http://www.jboss.org/products/jbosscache).
Segundos de Intervalo para Despertar	Especifique o **intervalo de tempo (em segundos)** que a política de expulsão de cache aguarda antes de despertar para executar as seguintes ações: ◆ Processar os eventos no nó expulso ◆ Limpar o limite de tamanho e descartar nós
Máx. de Nós	Especifique o **número máximo de nós** permitido no cache. Para não ter limite, especifique: `0`
Segundos de Tempo de Operação	Especifique o **tempo ocioso (em segundos)** antes de o nó ser descartado. Para não ter limite, especifique: `0`

Essas configurações são *obrigatórias*, o que significa que deve haver um valor global para cada um e, opcionalmente, um valor local.

Para *anular* o valor global de uma configuração com um valor local, marque a caixa de seleção *Habilitar Local* para essa configuração. Em seguida, especifique o valor local. (Certifique-se de que todos os valores locais sejam *válidos*. Caso contrário, você não poderá gravar suas mudanças.)

Observação: Para as configurações em que Habilitar Local estiver desmarcada, os valores locais existentes serão apagados quando você gravar.

3. Clique em *Gravar*.
4. Quando estiver pronto para ativar suas configurações gravadas, *reinicie o aplicativo de usuário* nos servidores de aplicativos apropriados.

13.3.5 Configurações de cache para clusters

Esta seção informa como configurar o cache quando você executa o aplicativo de usuário do Identity Manager em um cluster de servidores de aplicativos. Você precisa saber o seguinte:

- Seção , “Como o cluster é implementado” na página 224
- “Como o cache funciona com um cluster” na página 224
- “Preparando o uso de um cluster” na página 224
- “Definindo configurações de cache para clusters” na página 225

Como o cluster é implementado

No aplicativo de usuário do Identity Manager, o suporte a cluster do cache é implementado por meio do *JGroups*. JGroups é uma arquitetura de cluster de código-fonte aberto que está incluída no JBoss Application Server, mas também é executada em outros servidores de aplicativos.

O *cluster do aplicativo de usuário* consiste em nós em uma rede que executam o JGroups e usam um *ID de Grupo* comum. Por padrão, o ID de Grupo fornecido para o cluster do aplicativo de usuário é um UUID parecido com este:

```
c373e901aba5e8ee9966444553544200
```

O UUID ajuda a garantir a exclusividade para que o ID de Grupo do cluster do aplicativo de usuário não entre em conflito com os IDs de Grupo de outros clusters em seu ambiente. Por exemplo, o próprio JBoss Application Server usa dois clusters do JGroups e *reserva os IDs de Grupo DefaultPartition e TreeCache* para eles.

Para saber mais sobre JGroups, vá até www.jboss.org/products/jgroups (http://www.jboss.org/products/jgroups).

Como o cache funciona com um cluster

Quando você inicia o aplicativo de usuário, as definições de configuração do cache do aplicativo determinam se devem participar de um cluster e replicar as mudanças do cache nos outros nós desse cluster. Se o cluster estiver habilitado, o aplicativo de usuário finalizará a replicação com o envio de *mensagens de invalidação de entrada de cache* em cada nó quando ocorrerem mudanças.

Preparando o uso de um cluster

São necessários duas etapas importantes para se usar cache em um cluster:

1. *Configurar o cluster do JGroups*

   Isso envolve instalar o JBoss Application Server para usar a configuração *todos* e distribuir o aplicativo de usuário do Identity Manager (IDM.war) em cada servidor do cluster, normalmente colocando-o no diretório *farm*.

2. *Habilitar o uso do cluster* nas definições de configuração do cache do aplicativo de usuário

   Consulte “Definindo configurações de cache para clusters” na página 225 (abaixo).

Definindo configurações de cache para clusters

Depois que um cluster estiver pronto para ser usado, você poderá especificar configurações para o suporte do cache em todo esse cluster.

Para definir configurações de cache para clusters:

1. Vá até a página *Cache*.
2. Na seção *Configuração de Cluster* da página, especifique *valores globais ou locais* para as seguintes configurações, conforme apropriado:

Configuração	O que fazer
Cluster Habilitado	Selecione **Verdadeiro** para replicar mudanças de cache nos outros nós do cluster especificado pelo ID de Grupo. Para não participar de um cluster, selecione **Falso**.
ID de Grupo	Especifique o ID de Grupo do cluster do JGroups em que você deseja participar. **Não é necessário mudar o** ID de Grupo padrão fornecido para o cluster do aplicativo de usuário, **a menos que você queira um cluster diferente**. Lembre-se de que os seguintes IDs de Grupo são reservados o uso do JBoss Application Server: DefaultPartition e TreeCache. **Dica:** Para ver o ID de Grupo em mensagens de registro, verifique se o nível do registro de cache (com.sssw.fw.cachemgr) está definido como Informações ou superior.
Propriedades de Cluster	Especifique a **pilha de protocolo** do JGroups para o cluster especificado pelo ID de Grupo. Essa configuração deve ser usada por **administradores experientes** que talvez precisem ajustar as propriedades do cluster. Se esse não é o seu caso, não mude a pilha de protocolo padrão. Para ver as atuais propriedades de cluster, clique em **ver**. Para obter detalhes sobre a pilha de protocolo do JGroups, vá até www.joss.org/wiki/Wiki.jsp?page=JGroups (http://www.jboss.org/wiki/Wiki.jsp?page=JGroups).

Para *anular* o valor global de uma configuração com um valor local, marque a caixa de seleção *Habilitar Local* para essa configuração. Em seguida, especifique o valor local.

Observação: Para as configurações em que Habilitar Local estiver desmarcada, os valores locais existentes serão apagados quando você gravar.

Verifique se *todos os nós* do cluster *especificam o mesmo* ID de Grupo e Propriedades de Cluster. (Para ver essas configurações para determinado nó, é preciso acessar a interface de usuário do Identity Manager em execução no nó - navegando até o URL da interface de usuário desse servidor - e exibir a página Cache.)

3. Clique em *Gravar*.
4. Quando estiver pronto para ativar suas configurações gravadas, *reinicie o aplicativo de usuário* nos servidores de aplicativos apropriados.

Ferramentas para a exportação e a importação de dados de portal

14

Este capítulo ensina a usar a página *Ferramentas* da *guia Administração* da interface de usuário do Identity Manager. Os tópicos incluem:

- Seção 14.1, "Sobre a exportação e a importação de dados de portal" na página 227
- Seção 14.2, "Exportando dados do portal" na página 228
- Seção 14.3, "Importando dados do portal" na página 230

Para obter informações gerais sobre como acessar e trabalhar com a guia Administração, consulte o Capítulo 6, "Usando a guia Administração" na página 131.

14.1 Sobre a exportação e a importação de dados de portal

Você pode usar a página Ferramentas para *exportar ou importar* conteúdo do portal (páginas e portlets) usado no aplicativo de usuário do Identity Manager. Esse conteúdo também é conhecido como o *estado de configuração do portal* e inclui:

- Páginas de container e compartilhadas (incluindo os portlets atribuídos de cada página, além das preferências e configurações de cada portlet)
- Registros de Portlet

As ferramentas de exportação e importação permitem que você transfira o estado de configuração de um portal (aplicativo de usuário) para outro, conforme necessário. É assim que essas ferramentas funcionam:

Ferramenta	Como ela funciona
Exportação de Dados do Portal	Gera descrições XML de um conjunto de páginas de container e páginas compartilhadas selecionadas e portlets. Os arquivos XML são armazenados em um **arquivo ZIP da Exportação de Dados do Portal** que pode ser usado como fonte de informações da ferramenta Importação de Dados para o Portal.
Importação de Dados para o Portal	Aceita um arquivo ZIP da Exportação de Dados do Portal como fonte de informações. Use esse arquivo para gerar páginas de container e páginas compartilhadas e portlets em um portal (aplicativo de usuário).

14.1.1 Usos

Você pode usar as ferramentas para a exportação e importação de dados do portal para:

- *Mover* o estado de configuração do portal de um ambiente de teste (origem) para um ambiente de produção (destino)
- *Atualizar* o estado de configuração de um portal em incrementos

- *Clonar* um portal
- Opcionalmente, *sobregravar* o estado de configuração no portal de destino

14.1.2 Requisitos

Para usar as ferramentas de exportação e importação de dados do portal, verifique se o aplicativo de usuário do Identity Manager (portal) está *distribuído e em execução* nos servidores de aplicativos de origem e de destino.

Não é necessário que os servidores de origem e de destino acessem o mesmo *cofre de identidade*. Eles podem acessar outros, se apropriado. Os *usuários, grupos e containers* desses cofres de identidade *não precisam* ser iguais.

14.1.3 Restrições

Você *não pode* usar as ferramentas para a exportação e importação de dados do portal para:

- Exportar ou importar o estado de configuração do portal quando um servidor estiver atendendo a solicitações do usuário
- Exportar ou importar recursos e classes do portal
- Exportar ou importar recursos e classes do portlet
- Exportar ou importar dados de identidade e de aprovisionamento usados em um portal
- Exportar ou importar configurações de administração a não ser para páginas e portlets
- Migrar o estado de configuração de uma versão mais antiga do portal para outra mais recente (os portais devem ser da mesma versão)

14.1.4 Etapas

Para exportar e a importar dados de portal:

1. Se você executar uma atualização incremental, *faça backup* do portal de destino.
2. No portal de origem, *exporte* os dados do portal usando a ferramenta Exportação de Dados do Portal.

   Consulte a Seção 14.2, “Exportando dados do portal” na página 228.)
3. No portal de destino, *importe* os dados do portal usando a ferramenta Importação de Dados para o Portal.

   Consulte a Seção 14.3, “Importando dados do portal” na página 230.)
4. *Teste* o portal de destino para garantir que os dados importados sejam os esperados.

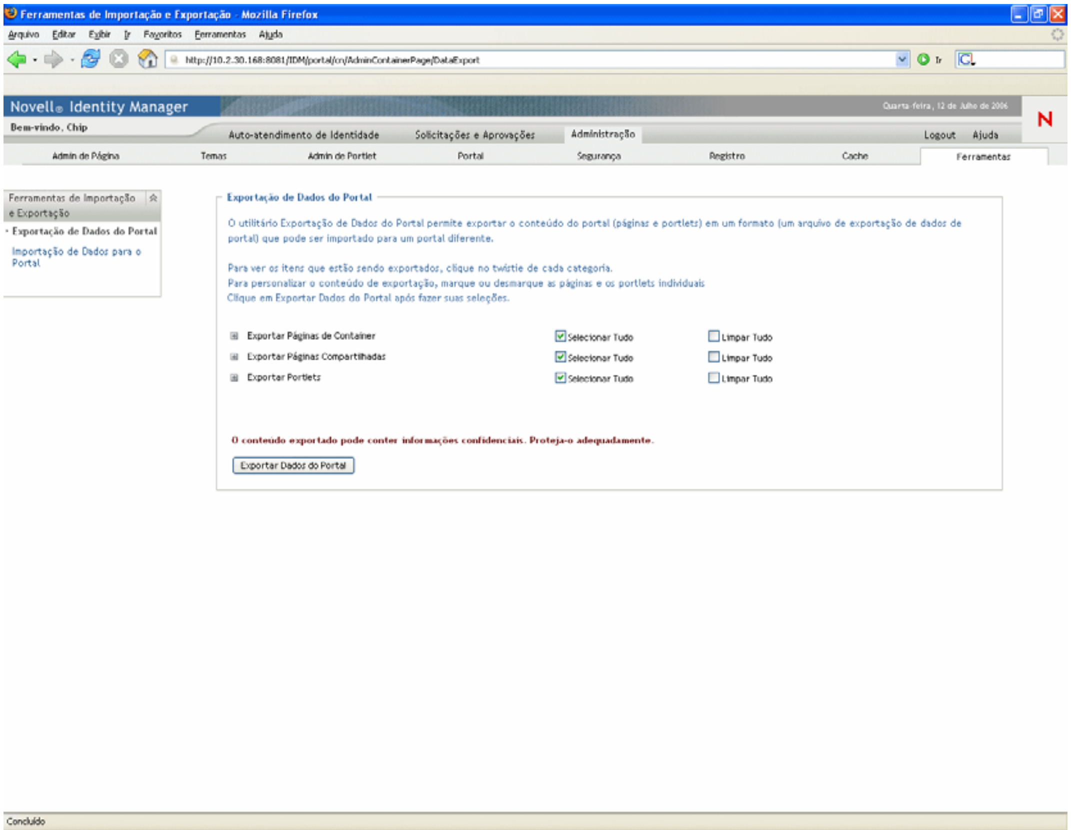
14.2 Exportando dados do portal

Esta seção descreve como exportar o estado de configuração de um portal para um arquivo ZIP da Exportação de Dados do Portal.

Para exportar dados do portal

1. Na página Ferramentas, selecione *Exportação de Dados do Portal* no menu de navegação à esquerda.

O painel Exportação de Dados do Portal é exibido:



2 Siga as instruções da tela para *selecionar as páginas do portal e os portlets* que serão exportados.

Observação: Mesmo os portlets que não foram selecionados poderão ser exportados. Se você exportar uma página que contém um portlet, mas não selecionar esse portlet para exportação, o portlet será exportado (para que nenhum erro de tempo de execução ocorra na página exportada).

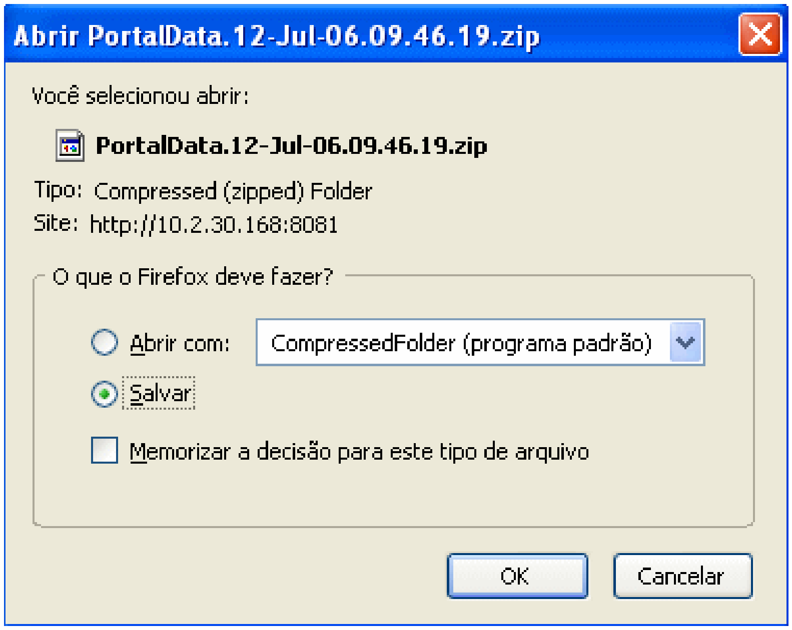
---

3 Depois de fazer suas seleções, clique no botão *Exportar Dados do Portal*.

Seu novo *arquivo ZIP da Exportação de Dados do Portal* é gerado, com um nome padrão que inclui a data e hora atuais. Por exemplo:

```
PortalData.21-Oct-05.09.12.16.zip
```

Você será solicitado a gravar esse arquivo ZIP localmente (ou abri-lo em um utilitário de arquivo adequado). Por exemplo:



4 *Grave* o arquivo ZIP da Exportação de Dados do Portal em um local apropriado.

14.3 Importando dados do portal

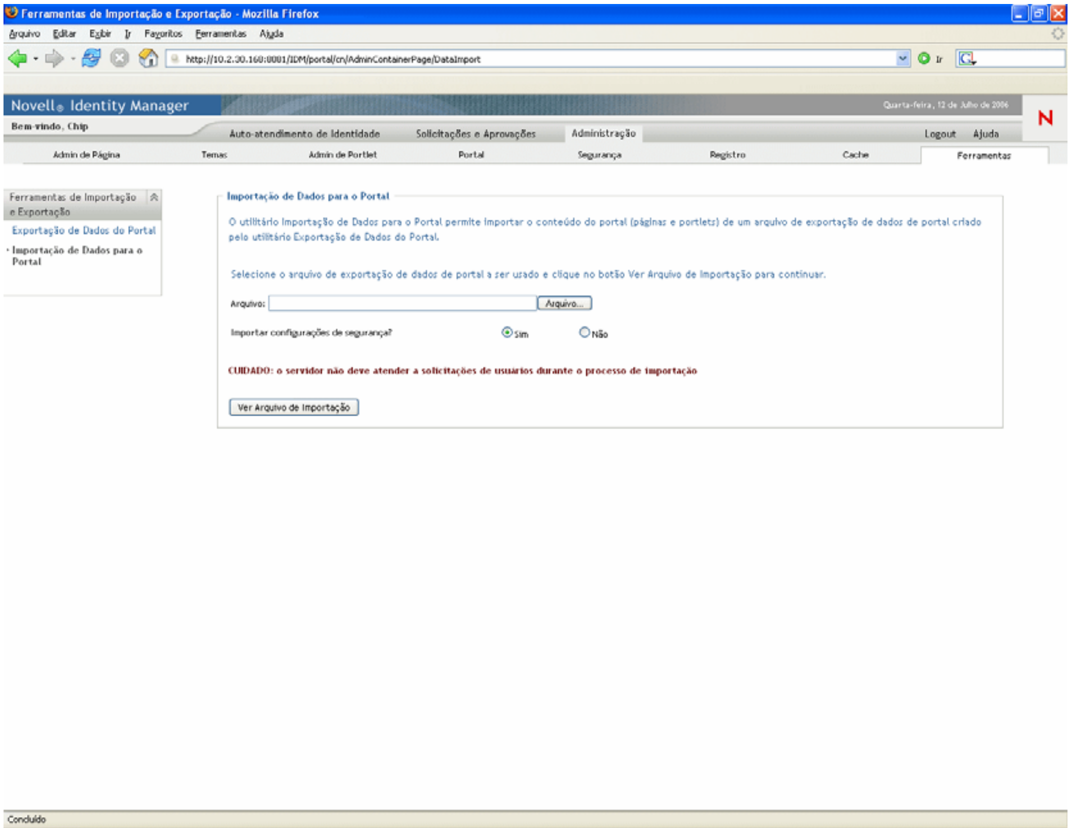
Esta seção descreve como importar o arquivo ZIP da Exportação de Dados do Portal para um portal.

Observação: Durante a importação, o servidor de aplicativos de destino deve estar em execução mas *não pode estar atendendo a solicitações do usuário*.

Para importar dados do portal:

1 Na página Ferramentas, selecione *Importação de Dados do Portal* no menu de navegação à esquerda.

O painel Importação de Dados do Portal é exibido:

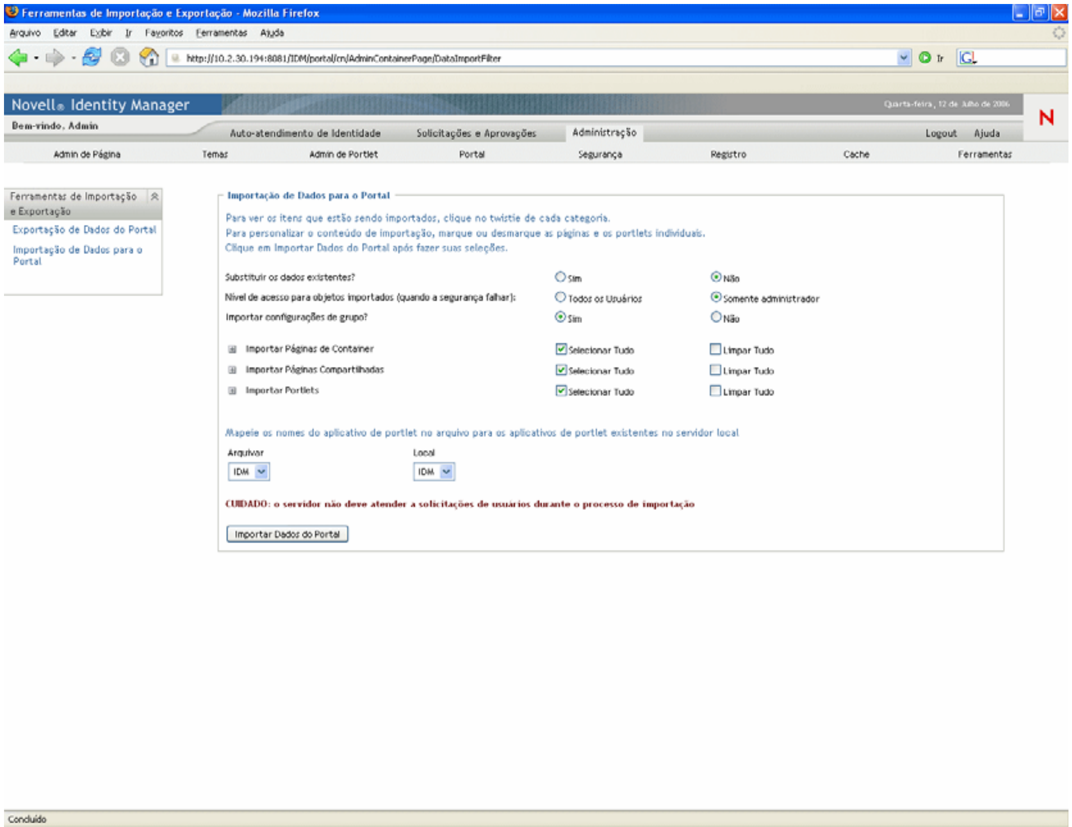


2 Especifique as seguintes *configurações gerais de importação*:

Configuração	O que fazer
Arquivar	Clique no botão **Pesquisar** para selecionar o **arquivo ZIP da Exportação de Dados do Portal** para importação. Por exemplo: `PortalData.21-Oct-05.09.12.16.zip`
Importar configurações de segurança?	Selecione uma das seguintes opções: ◆ **Sim** — Se você quiser importar as permissões que o arquivo ZIP da Exportação de Dados do Portal especifica para o acesso de usuários, grupos e containers a páginas e portlets. Certifique-se de que os usuários, grupos e containers envolvidos existam no cofre de identidade do portal de destino. Permissões para entidades ausentes não serão importadas. ◆ **Não** — Se você quiser ignorar as permissões especificadas pelo arquivo ZIP da Exportação de Dados do Portal.

3 Clique no botão *Ver Arquivo de Importação*.

O painel exibe mais especificações sobre o arquivo ZIP da Exportação de Dados do Portal e indica como importá-lo.



4 Especifique as seguintes *configurações detalhadas de importação*:

Configuração	O que fazer
Substituir os dados existentes?	Selecione uma das seguintes opções: ◆ **Sim** — Se você quiser que o conteúdo do arquivo ZIP da Exportação de Dados do Portal anule as páginas e os portlets correspondentes que já existem no portal de destino. Por exemplo, se o arquivo ZIP da Exportação de Dados do Portal contém uma página compartilhada denominada MyPage e o portal de destino contém uma página compartilhada também denominada MyPage, essa página será anulada no portal de destino. ◆ **Não** — Se você quiser ignorar a importação de todas as páginas e todos os portlets existentes.

<table>
<tr><th>Configuração</th><th>O que fazer</th></tr>
<tr><td>Nível de acesso para objetos importados</td><td>Selecione uma das seguintes opções:
◆ Todos os Usuários — Para ter acesso irrestrito a páginas e portlets importados.
◆ Somente administrador — Para ter acesso restrito a páginas e portlets importados.

Se você optar por importar as configurações de segurança, esse nível de acesso só será aplicado às páginas e aos portlets importados cuja configuração de segurança não tenha sido importada (normalmente porque determinados usuários, grupos ou containers não existem no cofre de identidade do portal de destino).

Se você optar por não importar as configurações de segurança, esse nível de acesso será aplicado a todas as páginas e todos os portlets importados.</td></tr>
<tr><td>Importar configurações de grupo?</td><td>(Se você optar por importar as configurações de segurança) Selecione uma das seguintes opções:
◆ Sim — Se você quiser importar as atribuições da página de container padrão e da página compartilhada padrão que o arquivo ZIP da Exportação de Dados do Portal especifica para os grupos. Certifique-se de que os grupos envolvidos existam no cofre de identidade do portal de destino. Atribuições para grupos ausentes não serão importadas.
◆ Não — Se você quiser ignorar as atribuições da página padrão que o arquivo ZIP da Exportação de Dados do Portal especifica para os grupos.</td></tr>
<tr><td>Importar Páginas de Container

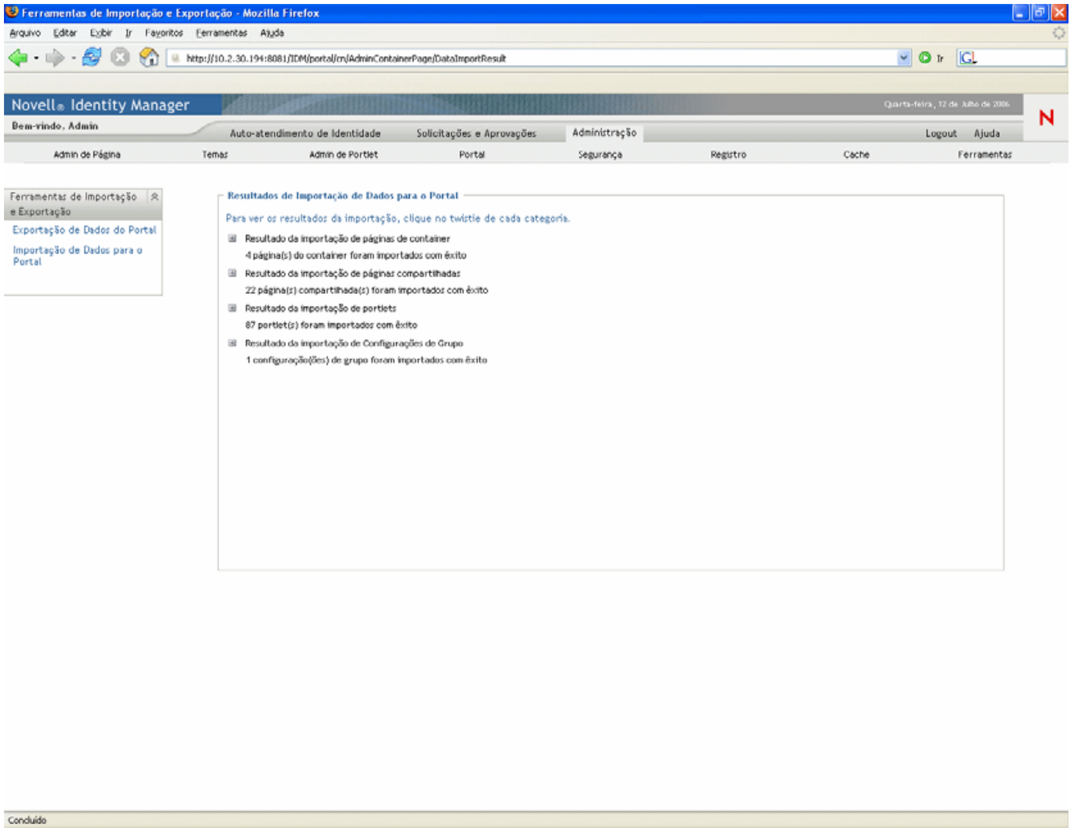
Importar Páginas Compartilhadas

Importar Portlets</td><td>Siga as instruções da tela para selecionar as páginas e os portlets que serão importados do arquivo ZIP da Exportação de Dados do Portal para o portal de destino.

Observação: Mesmo os portlets que não foram selecionados poderão ser importados. Se você importar uma página que contém um portlet, mas não selecionar esse portlet para importação, o portlet será importado (para que nenhum erro de tempo de execução ocorra na página importada).</td></tr>
<tr><td>Mapeie os nomes do aplicativo de portlet... Arquivar/Local</td><td>Use os menus suspensos Arquivar e Local para mapear os nomes de aplicativos de portlet no arquivo (ZIP da Exportação de Dados do Portal) para aplicativos de portlet existentes no servidor de aplicativos local (destino).</td></tr>
</table>

5 Quando você estiver pronto para iniciar a importação, clique no botão *Importar Dados para o Portal*.

Quando a importação estiver concluída, o painel *Resultado de Importação de Dados para o Portal* será exibido:



Importações incorretas são exibidas em vermelho. Para *solucionar problemas* de importação (ou exportação), consulte o console do sistema do servidor de aplicativos ou o arquivo de registro (como jboss/server/IDM/log/server.log) para verificar mensagens do seguinte *registro* do aplicativo de usuário:

```
com.novell.afw.portal.util
```

Referência de portlet

IV

Estes capítulos ensinam a configurar e identificar os portlets do sistema usados na interface de usuário do Identity Manager.

Sobre os portlets

15

Este capítulo fornece informações sobre os portlets usados no aplicativo de usuário do Identity Manager. Os tópicos incluem:

Para obter mais informações sobre como gerenciar portlets, consulte o Capítulo 9, "Administração de Portlet" na página 179.

15.1 Portlets adicionais

Os portlets adicionais oferecem diversos conjuntos de funções que podem ser adicionados ao aplicativo de usuário do Identity Manager. Os portlets adicionais têm funções de e-mail, sistema de arquivos e outras. Para obter mais informações:

Categoria de portlet	Para obter mais informações
E-mail Sistema de arquivos Miscelânea	Consulte o Identity Manager Accessory Portlet Administration Guide

15.2 Portlets Admin

Os portlets da categoria Admin são usados para controlar o layout e o conteúdo da interface de usuário.

Observação: É recomendável não usar ou modificar esses portlets. Eles oferecem os serviços de estrutura ao aplicativo de usuário.

Os portlets Admin incluem:

Nome do portlet	Descrição
Portlet de Cabeçalho	Exibe as informações de cabeçalho e os controles da guia de nível superior da interface de usuário. Não há preferências para este portlet.

Nome do portlet	Descrição
Navegação de Página Compartilhada	Exibe um menu que contém as páginas compartilhadas do aplicativo de usuário do Identity Manager. As preferências definem o que é exibido e como é exibido. Consulte a Seção 15.2.1, “Portlet Navegação de Página Compartilhada” na página 238.

15.2.1 Portlet Navegação de Página Compartilhada

O portlet Navegação de Página Compartilhada gera links para as páginas compartilhadas do aplicativo de usuário do Identity Manager. As configurações de preferência definem os links de página compartilhada que serão exibidos. As preferências incluem:

Preferência	O que especificar
sharedpages-sorting	A ordem em que as páginas compartilhadas são exibidas em uma categoria: Crescente e Decrescente
sharedpages-sortmode	Como classificar as páginas compartilhadas: Alfabética ou Prioridade.
sharedpages-category	Especifique uma ou mais das categorias de página compartilhada. O nome da categoria aparece como um cabeçalho com todas as páginas compartilhadas dessa categoria exibidas como links. A categoria não exibe páginas compartilhadas se não as contém. Se uma página compartilhada não estiver em uma categoria, ela aparecerá sem categoria.
guest-category	Especifique uma categoria cujos portlets você queira exibir na landing page do portal. Deve ser uma categoria que já exista, e as páginas contidas nessa categoria não podem ter qualquer restrição de leitura de ACL.

15.3 Portlets de Identidade

Os portlets de Identidade são usados pela guia Auto-atendimento de Identidade do aplicativo de usuário. Estão incluídos:

Nome do portlet	Descrição
Criar	Oferece uma interface à base de assistente que permite aos usuários criar objetos no cofre de identidade. Consulte o Capítulo 16, “Criar referência de portlet” na página 241.
Detalhe	Permite que os usuários exibam e manipulem os dados de atributo de uma entidade. Consulte o Capítulo 17, “Referência do portlet Detalhes” na página 247.

Nome do portlet	Descrição
Organograma	Permite que os usuários vejam e pesquisem os relacionamentos hierárquicos entre os objetos do cofre de identidade. Consulte o Capítulo 18, "Referência do portlet Organograma" na página 261.
Lista de Pesquisa	Permite que os usuários procurem objetos no cofre de identidade. Consulte o Capítulo 20, "Referência do portlet Lista de Pesquisa" na página 291.

15.4 Portlets de senha

Os portlets de senha oferecem a funcionalidade de auto-atendimento de senha ao aplicativo de usuário do Identity Manager. Estão incluídos:

Nome do portlet	Para obter mais informações
Resposta de Verificação do IDM	Consulte o Capítulo 19, "Referência dos portlets Gerenciamento de Senhas" na página 277.
Mudar Senha do IDM	
Senha do IDM Esquecida	
Definição de Dica do IDM	
Login do IDM	

15.5 Portlets do sistema

Os portlets do sistema oferecem serviços ao aplicativo de usuário do Identity Manager.

Observação: É recomendável não usar nem modificar os portlets dessa categoria.

Os portlets do sistema incluem:

Nome do portlet	Descrição
Controlador de Página do Portal	Exibe a página compartilhada selecionada por meio do portlet Navegação de Página Compartilhada. Não há preferências para este portlet.

Criar referência de portlet

16

Este capítulo ensina a usar o *portlet Criar* no aplicativo de usuário do Identity Manager. Os tópicos incluem:

- Seção 16.1, "Sobre o portlet Criar" na página 241
- Seção 16.2, "Configurando o portlet Criar" na página 242
- Seção 16.3, "Definindo preferências de criação" na página 244

16.1 Sobre o portlet Criar

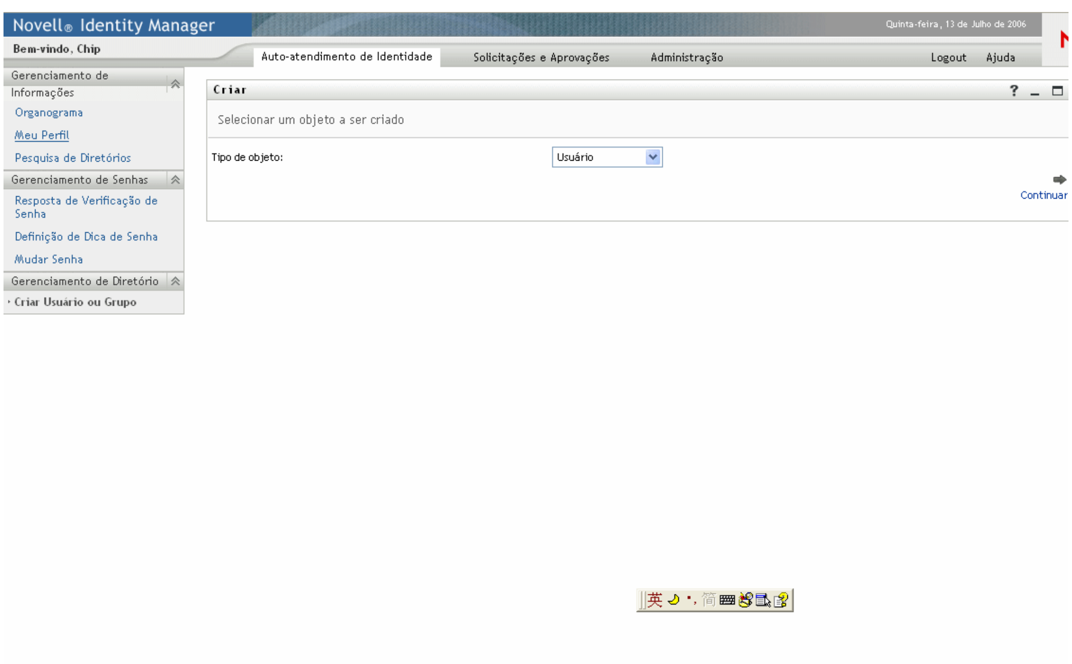
O portlet Criar contém um assistente fácil de usar que permite criar objetos do cofre de identidade de diversos tipos. Controle de preferências de portlet:

- Os tipos de objetos que o usuário pode criar.
- Os atributos que o usuário pode especificar.

Para obter mais informações, consulte a Seção 16.3, "Definindo preferências de criação" na página 244.

A configuração padrão do portlet Criar (que é acessado por meio da ação *Criar Usuário ou Grupo* do aplicativo de usuário do Identity Manager) permite aos usuários criar um Usuário, um Grupo ou um Grupo de Tarefas. O portlet é restrito, por padrão, ao Administrador de Aplicativo de Usuário. O seguinte exemplo mostra como o assistente do portlet Criar solicita ao usuário para:

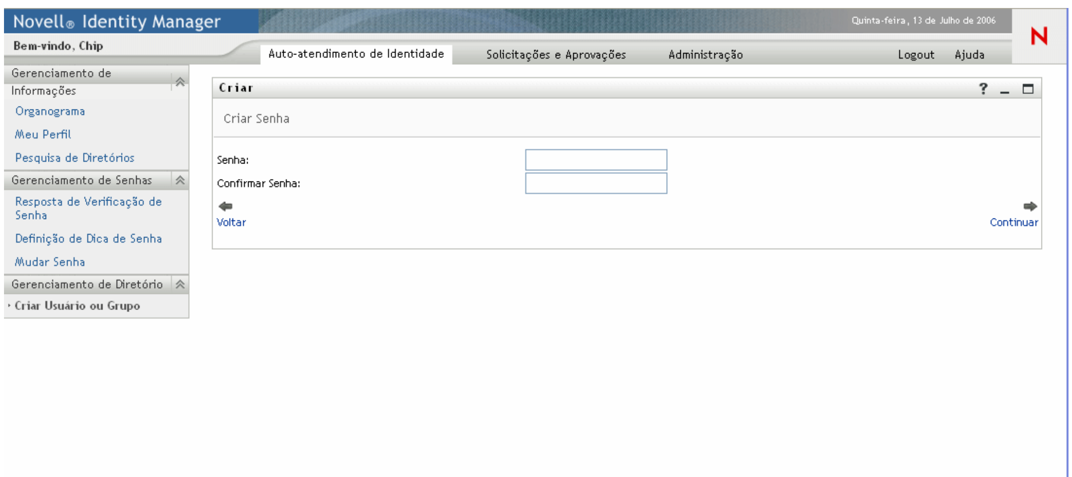
- *Selecionar o tipo de objeto* a ser criado:



- *Preencher os atributos do objeto*:



- *Solicitar uma senha*, quando o tipo de objeto exigir:



Se houver uma política de senha atribuída, todas as mensagens de política personalizadas serão exibidas pelo portlet.

- *Fornecer uma mensagem informativa* quando o objeto for criado corretamente, para estabelecer um link com o portlet Detalhes desse objeto (supondo que o portlet Detalhes esteja configurado da mesma forma) para maiores edições.

16.2 Configurando o portlet Criar

Para configurar o portlet Criar, será preciso:

Etapa	Tarefa	Descrição
1	Decidir se o recurso Criar Usuário ou Grupo atende às suas necessidades	Se atender, não haverá necessidade de ações adicionais. Se não atender, será preciso seguir as etapas restantes.
2	Definir os tipos de objetos que os usuários poderão criar	Adicione os objetos e os atributos à camada de abstração do diretório. Para obter mais informações, consulte Capítulo 4, "Configurando a Camada de Abstração do Diretório" na página 75.
3	Determinar como os usuários devem acessar esse novo portlet	Os usuários poderão iniciar o portlet em uma página nova ou uma página existente? Que usuários podem acessar o portlet e a página? Para obter mais informações sobre páginas, consulte o Capítulo 7, "Administração de Página" na página 137.
4	Especificar os usuários que têm acesso à página e à instância do portlet	Edite a segurança da página e adicione os usuários à lista. Para obter mais informações sobre como restringir o acesso do usuário às páginas, consulte o Capítulo 7, "Administração de Página" na página 137. Editar a instância do portlet para mudar a segurança. Para obter mais informações sobre como restringir o acesso do usuário aos portlets, consulte o Capítulo 9, "Administração de Portlet" na página 179.
5	Definir preferências para o portlet	As preferências permitem definir: ◆ Os objetos que os usuários podem criar. ◆ Os atributos que serão especificados durante a criação. Para obter mais informações, consulte a Seção 16.3, "Definindo preferências de criação" na página 244.
6	Testar	Verifique se os objetos foram criados e se os atributos estão preenchidos corretamente.
7	Estabelecer os direitos apropriados e efetivos no eDirectory para os usuários finais	Para criar um objeto, o usuário precisará ser **Trustee** da unidade organizacional e da organização em que o objeto foi criado.

16.2.1 Configuração da camada de abstração do diretório

Os objetos que podem ser criados e os atributos que podem ser preenchidos pelos usuários do portlet Criar devem ser definidos na camada de abstração do diretório da seguinte maneira:

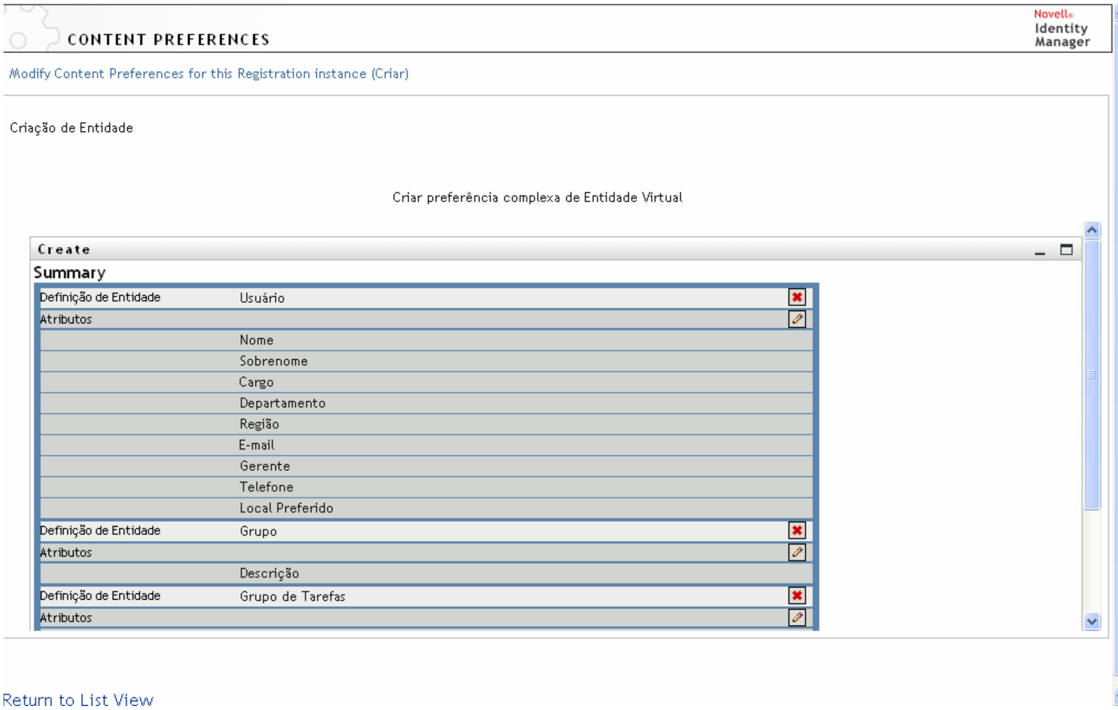
Tipo de definição	Propriedade	Valor
entidade	criar	Selecionada
	exibir	Selecionada Se não for selecionada, a entidade não será exibida na lista de entidades que podem ser criadas.
	Container de Criar	Especifique um container válido para o cofre de identidade. Se um container válido não for especificado, o container da raiz determinado durante a instalação do aplicativo de usuário será usado.
	Senha	Selecionada, se o tipo de entidade exigir uma senha ao ser criada. Qualquer um que tenha acesso ao portlet Criar e que tenha direitos de Trustee em relação à OU poderá criar e atribuir a **senha inicial**. Quando o novo usuário efetua login pela primeira vez, ele é redirecionado para o portlet Mudar Senha do IDM onde ele poderá modificar a senha inicial. Para obter mais informações sobre o portlet Mudar Senha do IDM, consulte o Capítulo 15, “Sobre os portlets” na página 237.
atributo	habilitado	Selecionado
	visualizável	Se habilitado ou visualizável não estiver selecionado (falso), o atributo não poderá ser usado pelo portlet.

Para obter mais informações sobre como configurar a camada de abstração, consulte o Capítulo 4, “Configurando a Camada de Abstração do Diretório” na página 75.

16.3 Definindo preferências de criação

Você pode configurar os tipos de objetos que o usuário pode criar e os atributos permitidos ou necessários às preferências de configuração.

As preferências do portlet Criar estão contidas em uma página de preferências personalizada. Quando aberta, as preferências individuais de Criar são exibidas:



As preferências estão descritas abaixo (você também pode clicar no botão Descrições para exibir a ajuda online do portlet).

Preferência	Descrição
Definição de Entidade	O nome do tipo de objeto a ser criado. Representa o início de um bloco de definição de identidade em que você define como o portlet tratará a operação de criar. **Para restringir objetos:** Os objetos relacionados nas preferências complexas são exibidos em uma lista suspensa. Para restringir os objetos que os usuários podem criar, remova-os da folha de preferências com o botão apagar. **Para adicionar outras entidades:** Clique em **Adicionar Definição de Entidade** e conclua o assistente.

Preferência	Descrição
Atributos	Controla os atributos que o usuário terá que preencher. É preciso incluir todos os atributos necessários dos objetos ou a criação do objeto falhará. Além disso, as preferências não serão gravadas corretamente se faltar algum atributo necessário. **Para adicionar ou remover um atributo:** ◆ Clique no botão Modificar Atributos.  ◆ Para adicionar um atributo, selecione-o (na lista de atributos disponíveis). Para selecionar vários atributos, use as teclas CTRL ou Shift. ◆ Clique na seta para movê-lo para a lista Selecionado. Faça o inverso para remover um atributo. ◆ Para reordenar a lista de atributos, clique nas setas para cima e para baixo à direita da lista Selecionado. Clique em **Submeter**. **Atributos e tipos de dados:** O tipo de dados do atributo afeta a maneira como ele é exibido. Por exemplo, se um atributo está definido como um subtipo da lista Local ou Global, ele será exibido em uma caixa de listagem. Para obter mais informações, consulte a Seção 4.3, “Trabalhando com entidades e atributos” na página 87.

Preenchendo o painel de preferências Para verificar se você enviou as entradas válidas, clique em *Submeter*. Se uma entrada não é válida, você verá uma mensagem de erro na parte superior da página de preferências. Clique em *Retorne à Tela de Lista* quando puder clicar em *Submeter* e nenhum erro ocorrerá. Clique em *Gravar Preferências* depois de retornar à Tela de Lista.

Referência do portlet Detalhes

17

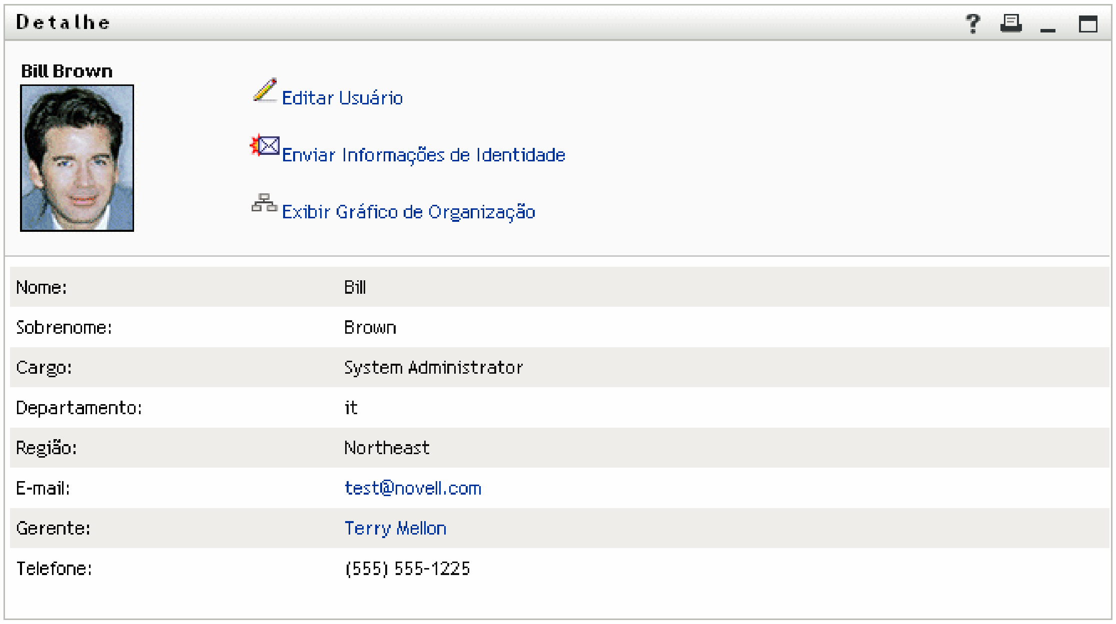
Este capítulo informa sobre o *portlet Detalhes* que permite aos usuários exibir e manipular os dados de atributo de uma entidade. É a base da ação Meu Perfil na guia Auto-Atendimento de Identidade do aplicativo de usuário do Identity Manager. Os tópicos incluem:

17.1 Sobre o portlet Detalhes

O portlet Detalhes oferece aos usuários uma tela detalhada dos atributos da entidade e respectivos valores. O portlet tem dois modos: exibir e editar. Ao acessar o portlet Detalhes, os usuários podem aproveitar seus recursos internos e trabalhar com suas informações, inclusive:

17.1.1 Exibindo dados de entidade

Quando acessado, o portlet Detalhes exibe *dados de atributo sobre uma entidade selecionada*, como um usuário ou grupo. Por exemplo, esta é a provável exibição do portlet Detalhes quando o usuário Bill Brown verifica suas próprias informações:



Imagens do usuário Por padrão, o portlet Detalhes é configurado para incluir o atributo Fotografia do Usuário. Entretanto, se o cofre de identidade não incluir esse atributo ou se ele não for preenchido, uma imagem padrão será exibida em tempo de execução. Se você armazenar as imagens do usuário em outro local, poderá configurar o portlet para exibi-las.

Para obter mais informações, consulte "Carregando imagens dinamicamente" na página 251.

Determinando os atributos a serem exibidos

O portlet Detalhes só exibe os atributos que:

- As definições de dados da *camada de abstração do diretório* tornam disponíveis para exibição

  Para obter informações sobre configuração de VDD, consulte o Capítulo 4, "Configurando a Camada de Abstração do Diretório" na página 75.
- Estão especificados nas *preferências* de Detalhes

  Para informar-se sobre a especificação dos atributos que serão exibidos no portlet Detalhes, consulte a Seção 17.5, "Definindo preferências" na página 258.
- O usuário atual tem *direitos* de exibição

  Por exemplo, os gerentes com direitos ao atributo salário verão esse tipo de dados, mas outros usuários não.

  Para obter mais informações, consulte a Seção 17.2.2, "Atribuindo direitos a entidades" na página 256.
- Estejam preenchidos com um *valor*

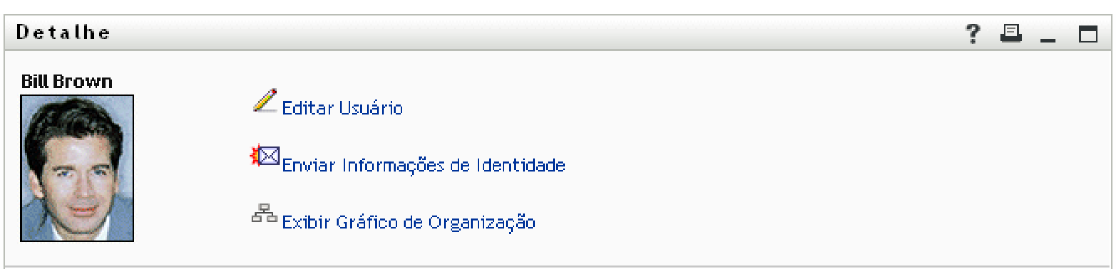
Determinando como os atributos serão exibidos

Ao exibir atributos, Detalhes *formata os dados como texto*, exceto nos seguintes casos:

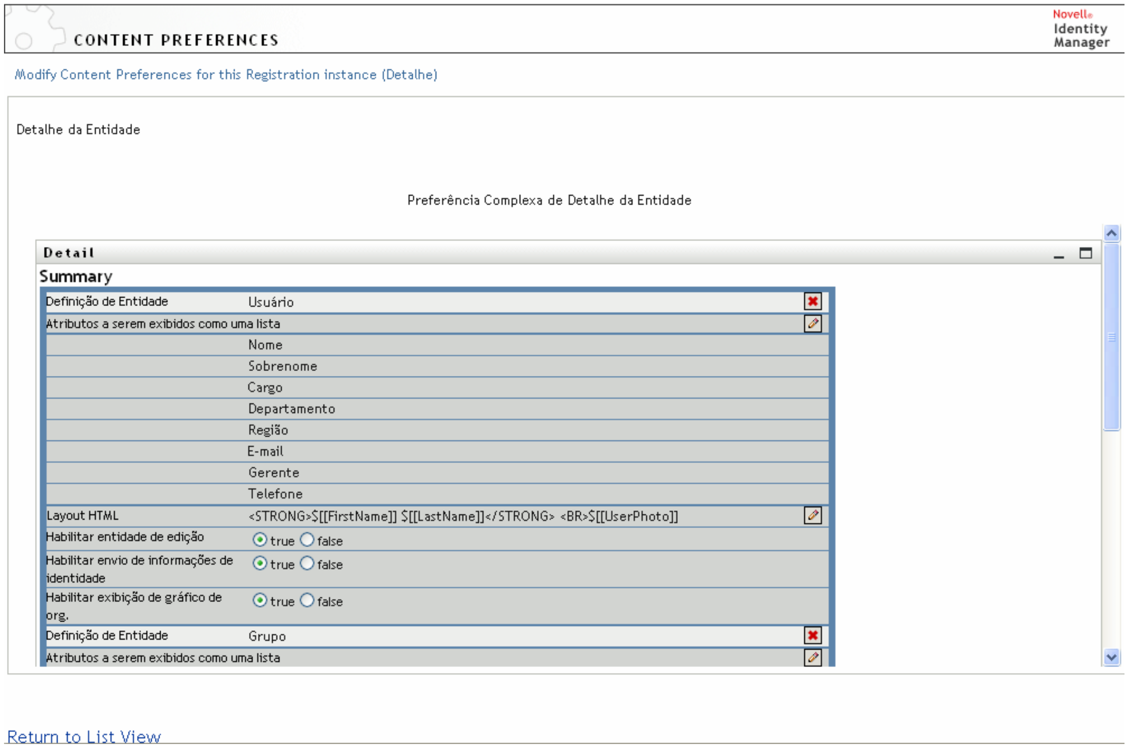
Especificação de formato na definição da camada de abstração	Como é exibido
Formato: e-mail	Como um link mail-to
Formato: ◆ groupwise-im ◆ aol-im ◆ yahoo-im	Como um ícone que inicia um bate-papo e adiciona o usuário
Tipo de dados: binário **Formato:** imagem	Como um botão e um link para visualizar a imagem
Tipo de dados: booleano	Como botões de opção desabilitados que indicam verdadeiro ou falso Os botões são exibidos sem indicar um valor padrão, pois o atributo não é de fato criado para o usuário até um valor ser especificado.
Multivalor: Selecionado	Como um conjunto repetido de controles para edição, adição e remoção de valores de atributo individuais (na forma de uma lista separada por vírgula)
Tipo de controle: DNLookup	Como um link No exemplo acima, um link (`Terry Mellon`) é exibido para o acesso aos dados de Detalhes do gerente de Bill Brown.
Tipo de controle: ◆ Lista Local ◆ Lista Global	Como a etiqueta de exibição, e não o valor real (chave) Por exemplo, o atributo EmployeeType exibe `Tempo Integral` em vez do valor real `ft`.

Determinando o que a área do cabeçalho exibe

Você pode criar um layout para a área do cabeçalho do portlet Detalhes com os recursos HTML padrão:



As preferências de Detalhes fornecem um *Editor de Layout HTML* que pode ser usado para criar a aparência e o conteúdo desejados:



Usando o Editor de Layout HTML

O Editor de Layout HTML tem os recursos típicos de um editor de HTML para definir a formatação do texto e das listas, e também especificar âncoras e imagens, entre outros.

Palavras-chave Ao criar seu layout, você pode usar a lista suspensa Palavras-chave para inserir variáveis na área do cabeçalho do portlet Detalhes que serão substituídas em tempo de execução por valores de atributo específicos. Você também pode digitá-las usando esta sintaxe:

```
$[[palavra-chave]]
```

Onde *palavra-chave* é o valor de um atributo como LastName.

Você pode concatenar atributos usando esta sintaxe:

```
$[[palavra-chave+palavra-chave]]
```

Por exemplo:

```
$[[FirstName+LastName]]
```

Você pode concatenar quantos atributos quiser e também incluir strings entre aspas como esta:

```
$[[palavra-chave+"exemplo de texto"+palavra-chave]]
```

Os valores das palavras-chave e do texto entre aspas serão processados.

Observação: Palavras-chave com erros ortográficos no layout serão renderizadas com tais erros em tempo de execução (incluindo $[[]]).

Carregando imagens dinamicamente Para exibir imagens, como fotografias do usuário, que estão armazenadas no cofre de identidade, é possível adicionar o nome do atributo com o Editor de Layout HTML. Por exemplo, a inclusão do atributo Fotografia do Usuário exibe a foto do usuário. Se você armazena imagens fora do cofre de identidade, precisará usar a tag IMG: (no *modo Exibir Origem* do Editor de HTML) da seguinte maneira:

1 Vá até as preferências do portlet e acesse o Editor de HTML.
2 Clique em *Exibir Origem*.
3 Use a tag IMG: para combinar um local, uma chave de atributo e uma extensão de arquivo usando uma sintaxe como esta:

```
$[[IMG:"URL" + atributo-chave-nome + "fileextension"]]
```

O exemplo a seguir mostra a sintaxe usada caso você tenha armazenado fotografias dos funcionários como imagens JPG de acordo com o Sobrenome no subdiretório /images do servidor de aplicativos:

```
$[[IMG:"http://myhost:8080/images/"+LastName+".jpg"]]
```

Em tempo de execução, o portlet concatena o URL com o atributo LastName e a extensão de arquivo .jpg.

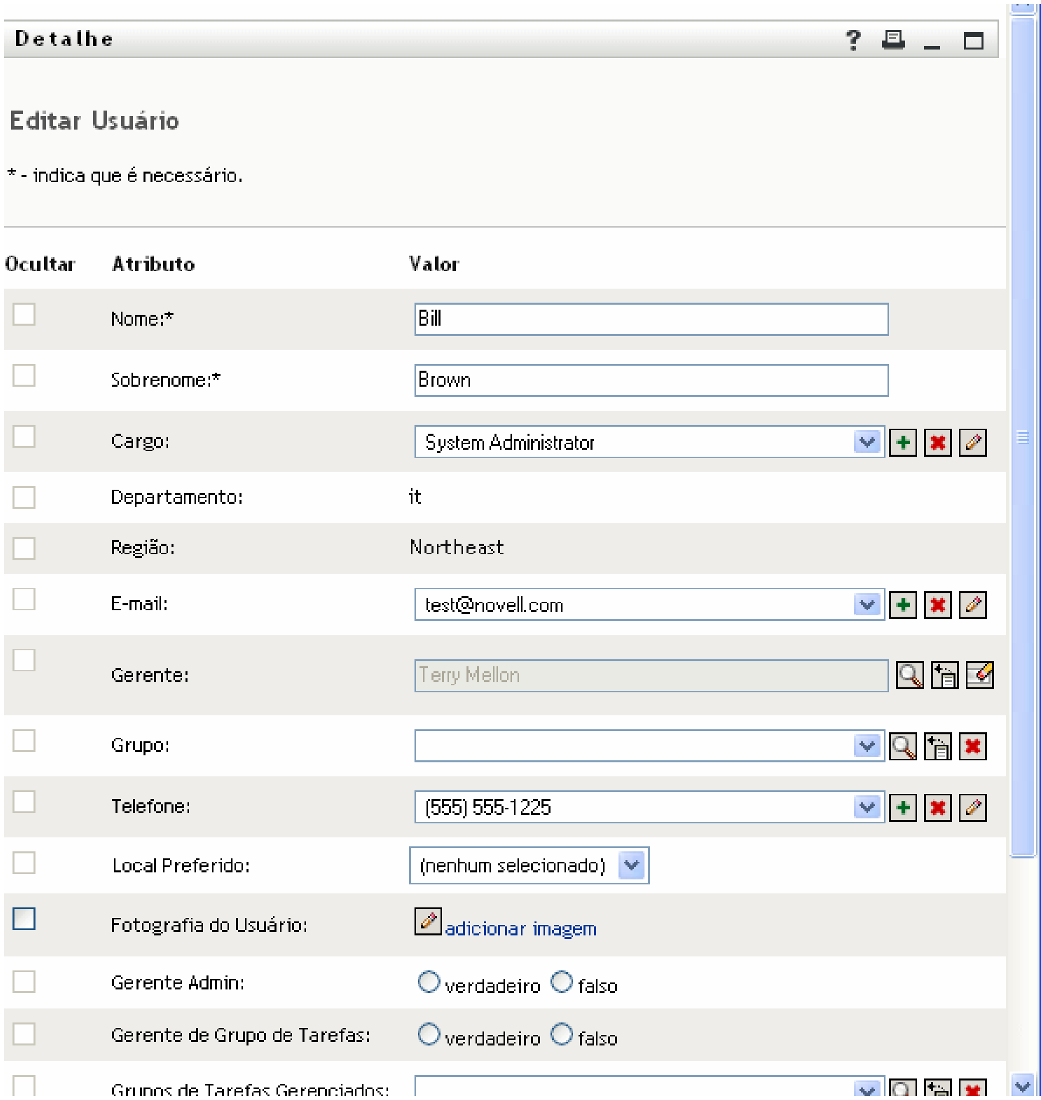
Lembre-se de que o Editor de HTML oferece suporte a uma sintaxe flexível. Ele aceita qualquer combinação de texto e atributos de forma que se obtenha uma sintaxe como:

```
$[[IMG:"qualquer texto" + atributo-chave-nome + ...]]
```

17.1.2 Editando dados de entidade

O portlet Detalhes fornece automaticamente um link *Editar* (como *Editar suas Informações* ou *Editar Usuário* ou *Editar Dispositivo*) para alternar do modo de exibição para o modo de edição. Com isso, os usuários que têm os direitos apropriados para a entidade podem mudar os valores de seus atributos e gravar essas mudanças.

Por exemplo, o portlet Detalhes pode exibir o seguinte quando o usuário Bill Brown (que tem os direitos necessários) edita suas próprias informações:



Observação: Quando os botões de opção dos atributos booleanos estão desmarcados, o atributo não existe para o usuário. Marcar o botão de opção *verdadeiro* ou *falso* criará o atributo para o usuário e definirá seu valor.

Determinando os atributos a serem exibidos

No modo de edição, o portlet Detalhes exibe somente os atributos que:

- As definições de dados da *camada de abstração do diretório* tornam disponíveis para exibição

  Para obter mais informações sobre definições de dados, consulte o Capítulo 4, “Configurando a Camada de Abstração do Diretório” na página 75.

- O usuário atual tem *direitos* de exibição

Por exemplo, os gerentes com direitos ao atributo salário verão esse tipo de dados, mas outros usuários não.

Para obter mais informações, consulte a Seção 17.2.2, “Atribuindo direitos a entidades” na página 256.

Um atributo deve atender a todos os critérios acima para aparecer no modo de edição.

Determinando como os atributos serão exibidos

No modo de edição, o portlet Detalhes formata todo atributo editável como uma *caixa de texto*, exceto nos seguintes casos:

Especificação do tipo de atributo (em arquivos VDD)	Como é exibido
Tipo de dados: binário Formato: imagem	Como um botão e um link para o portlet Entity Image Upload para ver, atualizar ou adicionar a imagem
Tipo de dados: booleano	Como botões de opção que indicam verdadeiro ou falso
hide:Selected	Como uma caixa de seleção Ocultar
multivalue=Selected	Como um conjunto de controles para editar, adicionar e remover valores de atributo
Tipo de controle: DNLookup	Como um botão para iniciar o portlet Lista de Parâmetros para procurar e selecionar DN
Tipo de controle: ◆ Lista local ◆ Lista global	Como uma lista suspensa (que permite diversas seleções, se for aplicável)

Os atributos que não podem ser editados (por definição ou devido a direitos do usuário inadequados) são exibidos como *desabilitados* ou *apenas leitura*.

Validando mudanças

Durante a edição, a validação de dados é realizada automaticamente para as seguintes especificações de tipo de atributo:

- Formato: e-mail
- Tipo de dados: número inteiro
- Tipo de controle: faixa

Quando se usa um tipo de controle de lista local ou global, é possível que a lista exibida inclua valores que estão fora dos limites especificados do atributo. Entretanto, esses valores serão marcados como fora de faixa, e a validação impedirá que sejam enviados.

Definindo uma entidade Meu Perfil padrão

Ao definir uma entidade na camada de abstração do diretório, você pode especificar um valor para *Entidade Meu Perfil Padrão* (no elemento Configuração do editor da camada de abstração do diretório) para determinar que outra definição de entidade seja usada para edição. Quando você

alterna do modo de exibição para o modo de edição, o portlet Detalhes verifica se esse elemento está especificado e usa a definição de entidade apropriada para apresentar os atributos.

Por exemplo, suponha que a definição de entidade Estudante inclua *usuário* como o valor de *Entidade Meu Perfil Padrão*. Nesse caso, o modo de exibição usará a definição de entidade Estudante, mas o modo de edição utilizará a definição de entidade usuário.

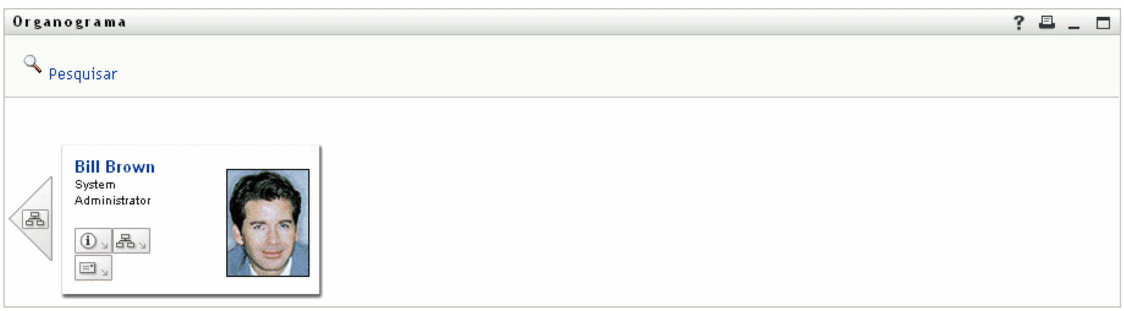
17.1.3 Enviando dados de entidade por e-mail

O portlet Detalhes fornece automaticamente um link chamado *Enviar Informações de Identidade*. Os usuários podem clicar nesse link para enviar o URL de Detalhes da entidade por e-mail para um ou mais usuários. O envio por e-mail do URL de Detalhes em vez das informações mantém a segurança, pois quem receber o URL precisará ter a autorização apropriada para usá-lo.

17.1.4 Vinculando a um organograma

O portlet Detalhes fornece automaticamente um link chamado *Exibir Gráfico de Organização*. Os usuários podem clicar nesse link para exibir o portlet Organograma da entidade.

Por exemplo, se você estiver visualizando Detalhes do usuário Bill Brown e clicar nesse link, verá:

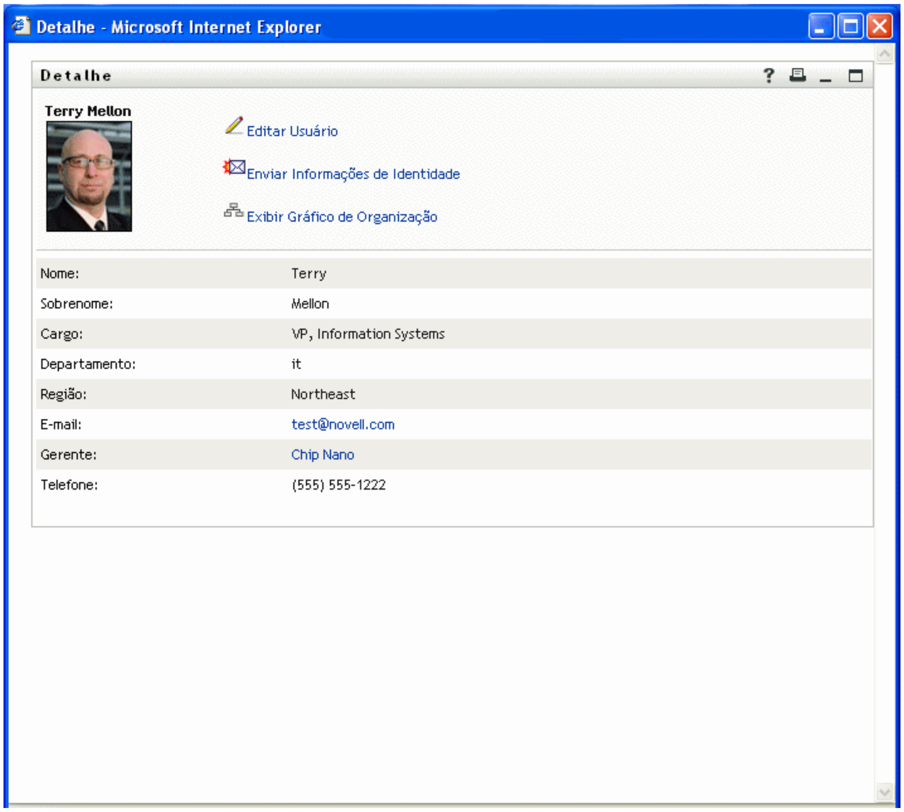


Para obter mais informações sobre o portlet Organograma, consulte o Capítulo 15, "Sobre os portlets" na página 237.

17.1.5 Criando links para detalhes de outras entidades

Quando você configura o portlet Detalhes, pode ser conveniente que os usuários se vinculem a entidades relacionadas à atual. Para fazer isso, você pode incluir atributos que são definidos (na camada de abstração do diretório) com o *tipo de controle DNLookup*.

Quando o atributo Gerente é exibido nos Detalhes de um usuário, ele aparece como um *link*. O link exibirá Detalhes do Gerente.



Para obter mais informações sobre a camada de abstração do diretório, consulte o Capítulo 4, “Configurando a Camada de Abstração do Diretório” na página 75.

Para informar-se sobre a especificação dos atributos que serão exibidos no portlet Detalhes, consulte a Seção 17.5, “Definindo preferências” na página 258.

17.1.6 Imprimindo dados de entidade

Por padrão, as configurações de exibição do portlet Detalhes habilita a opção *Imprimir* na barra de título do portlet. Se você mantiver a opção Imprimir habilitada, os usuários poderão clicar nela para exibir uma versão com formato para impressão do conteúdo de Detalhes:

Para mudar essa ou outras configurações do portlet Detalhes, use a guia Administração para atualizar o Registro de Portlet de *DetailPortlet* (na página Administração de Portlet).

Para obter mais informações, consulte o Capítulo 9, “Administração de Portlet” na página 179.

17.2 Pré-requisitos

Antes de usar o portlet Detalhes, é importante informar-se sobre:

- Seção 17.2.1, “Configurando a camada de abstração do diretório” na página 256
- Seção 17.2.2, “Atribuindo direitos a entidades” na página 256

17.2.1 Configurando a camada de abstração do diretório

O portlet Detalhes depende das definições da *camada de abstração do diretório* de várias maneiras. Nas próximas seções deste capítulo, há instruções sobre como configurar as definições dos dados da camada de abstração do diretório para dar suporte a recursos específicos do portlet Detalhes:

- Seção 17.1.1, "Exibindo dados de entidade" na página 248
- Seção 17.1.2, "Editando dados de entidade" na página 251
- Seção 17.4, "Usando Detalhes em uma página" na página 258

Para obter informações sobre configuração, consulte o Capítulo 4, "Configurando a Camada de Abstração do Diretório" na página 75.

17.2.2 Atribuindo direitos a entidades

Para ter acesso a uma entidade e seus atributos no portlet Detalhes, os usuários devem ter os *direitos apropriados atribuídos no eDirectory*:

Para	O usuário precisa deste direito
Exibir um atributo	Ler
Editar um atributo	Gravar

Para atribuir direitos, você precisa especificar que o usuário é um *trustee* de um objeto (entidade). Em seguida, você pode especificar os direitos que serão definidos para os atributos.

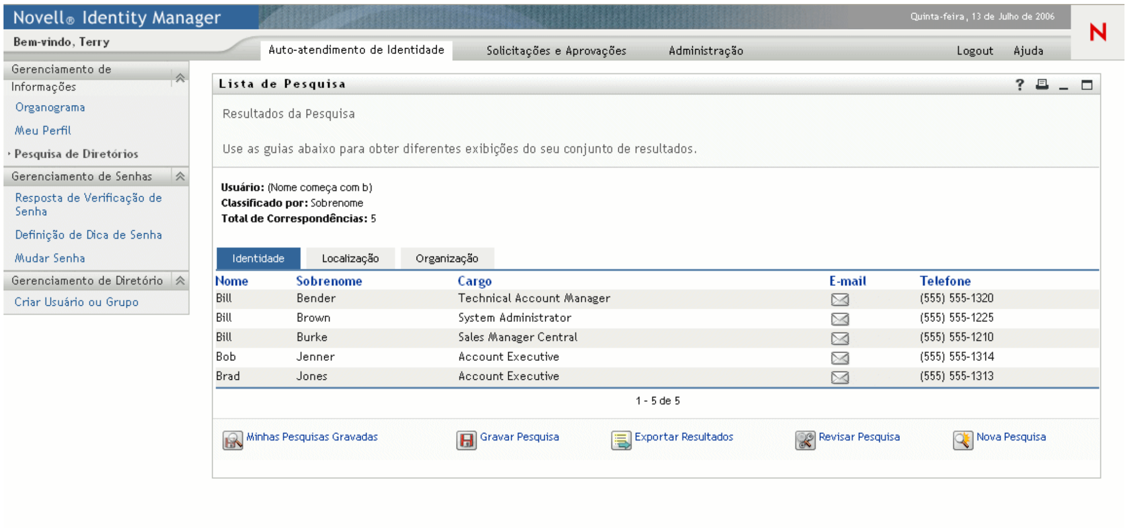
17.3 Iniciando Detalhes em outros portlets

É comum iniciar o portlet Detalhes depois de selecionar uma entidade em um dos outros portlets de identidade. Você pode iniciar Detalhes:

- Seção 17.3.1, "No portlet Lista de Pesquisa" na página 257
- Seção 17.3.2, "No portlet Organograma" na página 257

17.3.1 No portlet Lista de Pesquisa

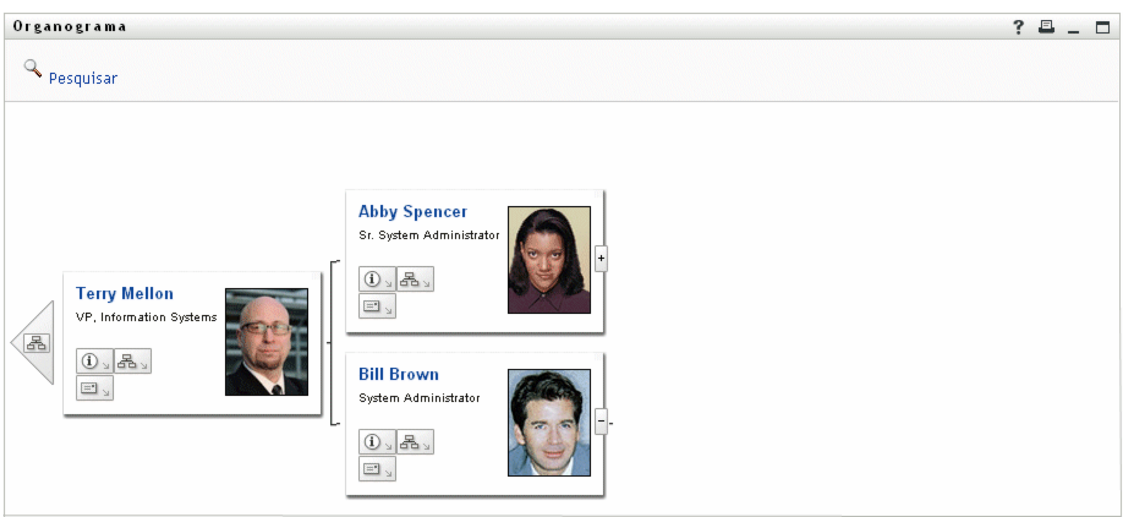
No portlet Lista de Pesquisa, os usuários podem *clicar em uma linha de entidade* nos resultados da pesquisa para exibir os Detalhes daquela entidade. Por exemplo, clique na linha de Bill Brown na lista para exibir o portlet de Detalhes com os dados de atributo desse usuário:



Para obter mais informações sobre o portlet Lista de Pesquisa, consulte o Capítulo 20, "Referência do portlet Lista de Pesquisa" na página 291.

17.3.2 No portlet Organograma

No portlet Organograma, os usuários podem clicar no *ícone de Ações de Identidade* de uma entidade e selecionar *Mostrar Informações* para exibir detalhes dessa entidade. Por exemplo, clique na linha em Mostrar Informações para Bill Brown no organograma para exibir o portlet Detalhes com os dados de atributo desse usuário:



Para obter mais informações sobre o portlet Organograma, consulte o Capítulo 15, "Sobre os portlets" na página 237.

17.4 Usando Detalhes em uma página

Se você quiser oferecer aos usuários recurso de auto-atendimento para exibição e possivelmente edição de seus próprios dados de atributo, adicione o portlet Detalhes a uma *página compartilhada*. Quando usado em uma página compartilhada, o portlet Detalhes acessa automaticamente os dados do usuário atual (ou outra entidade padrão).

Por exemplo, o usuário Bill Brown pode efetuar login e ir para a seguinte página pessoal para manter suas próprias informações pelo portlet Detalhes:



Para determinar qual definição de entidade o portlet Detalhes deve usar na situação (em que ele é acessado em uma página, e não iniciado por outro portlet), especifique a configuração *Entidade 'Meu Perfil' Padrão* no elemneto Configuração da camada de abstração do diretório.

17.5 Definindo preferências

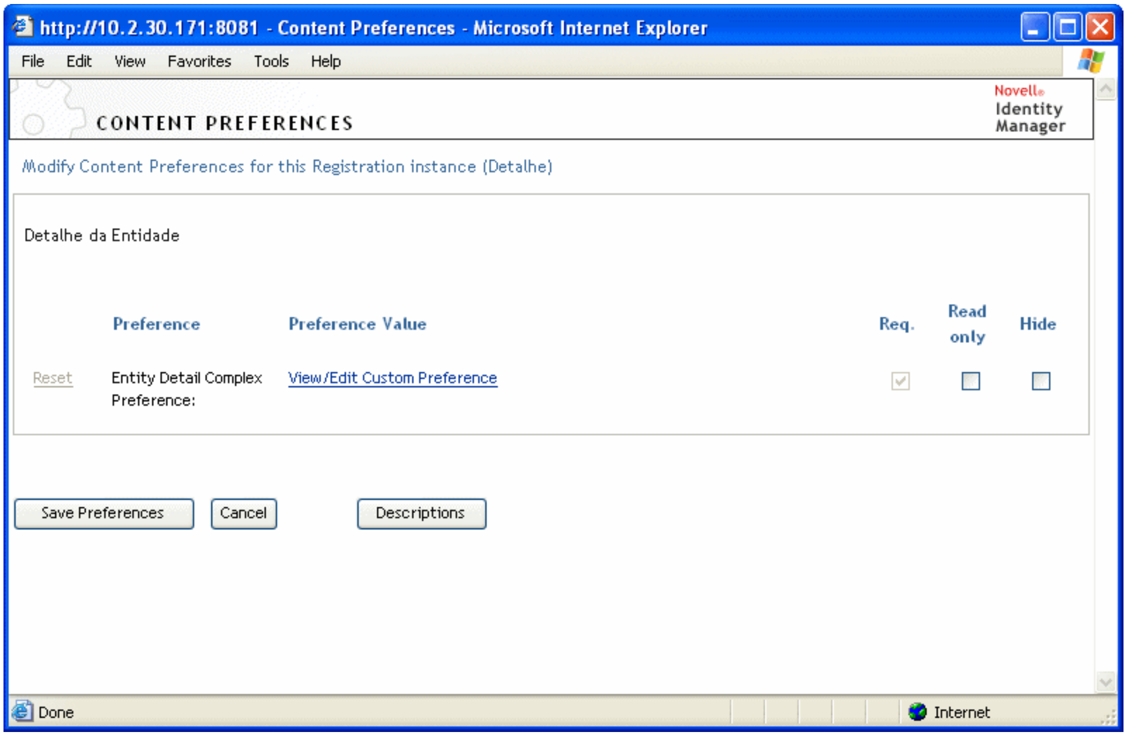
As preferências definem o conteúdo e a aparência do portlet Detalhes. A forma como você usa o portlet Detalhes determina onde as preferências devem ser definidas:

Para saber como acessar as preferências do portlet em páginas de container ou páginas compartilhadas, consulte o Capítulo 7, "Administração de Página" na página 137.

Para saber como acessar as preferências para um registro de portlet, consulte o Capítulo 9, "Administração de Portlet" na página 179.

17.5.1 Sobre as preferências

As preferências do portlet Detalhes estão contidas em uma *Preferência Complexa de Detalhe*.



Quando você abrir essa preferência complexa, as preferências individuais de Detalhes serão exibidas:



Essas preferências *aplicam-se apenas ao modo de exibição* (e não ao modo de edição). Elas incluem o seguinte:

Preferência	Detalhes
Definição de Entidade	Especifica a lista de atributos e o layout HTML a ser exibido quando Detalhes for usado para determinado tipo de entidade (como Usuário, Dispositivo ou Grupo). Você pode clicar em **Adicionar Definição de Entidade** para especificar o suporte de Detalhes a tipos adicionais de entidade.
Atributos a serem exibidos como uma lista	Especifica quais atributos da entidade selecionada o portlet deve exibir. Esses atributos serão relacionados na ordem que você escolher. Existe um botão para a adição ou remoção dos atributos.
Layout HTML	Fornece um botão para abrir o **Editor de Layout HTML**, onde você pode criar a área de cabeçalho que o portlet Detalhes exibirá para a entidade selecionada. Para obter detalhes, consulte “Determinando o que a área do cabeçalho exibe” na página 249.

Referência do portlet Organograma

18

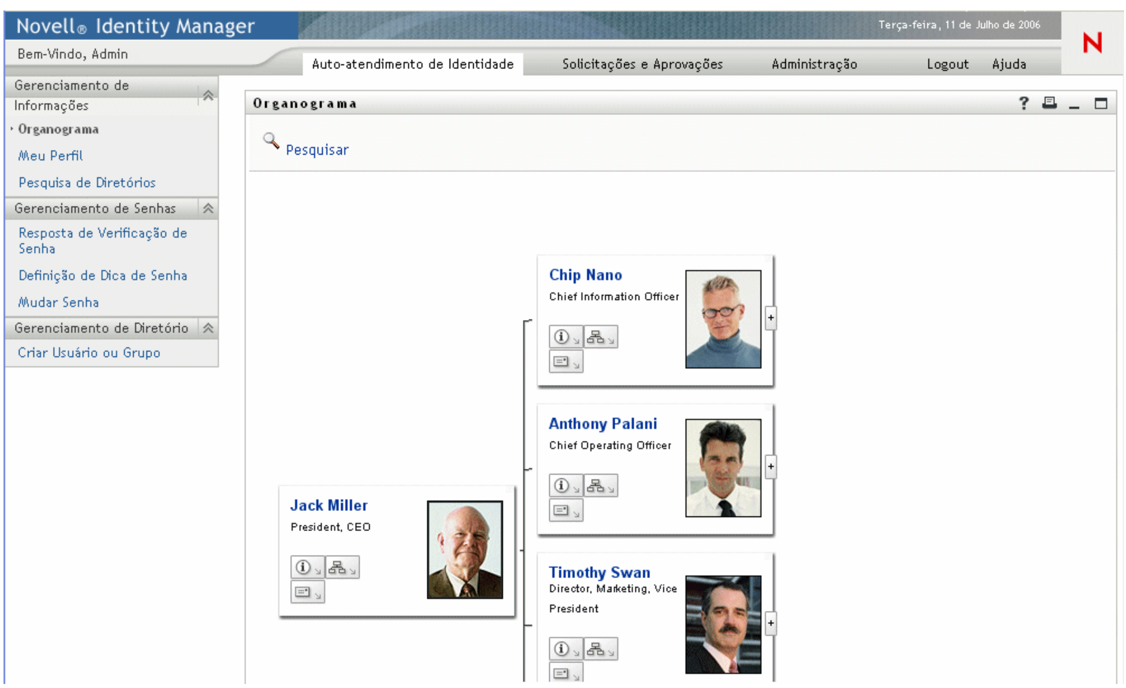
Este capítulo informa como modificar recursos de organograma ou adicionar novos ao aplicativo de usuário do Identity Manager. Os tópicos incluem:

18.1 Sobre o Organograma

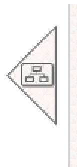
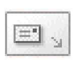
O portlet Organograma permite que os usuários finais vejam e pesquisem uma representação gráfica dos relacionamentos hierárquicos entre os objetos no cofre de identidade. Por exemplo, você pode definir portlets Organograma que indicam a hierarquia de:

- Uma organização (como funcionários e gerentes)
- A participação em um grupo (como todos os funcionários de um grupo)
- Dispositivos atribuídos a um usuário (como celulares e laptops)

A configuração padrão da guia Auto-atendimento de Identidade do aplicativo de usuário do Identity Manager inclui uma ação Organograma. Essa ação é um portlet Organograma configurado para mostrar os relacionamentos entre objetos do usuário no cofre de identidade. O seguinte exemplo mostra como o portlet Organograma padrão renderiza esse relacionamento (usando exemplo de dados).



Links internos O portlet Organograma inclui os links internos a seguir.

Link	Descrição
	Permite que o usuário navegue até o próximo nível superior. Isso só fica disponível quando você visualiza um relacionamento em que as entidades pai e filho são iguais.
	Inicia o portlet Detalhes. Esse link interno pode ser configurado nas preferências de layout de organograma descritas em “Preferências de layout de organograma” na página 269
	Exibe uma lista de organogramas. Permite que os usuários escolham um organograma para visualização. Essa é uma lista dinâmica de organogramas. Ela exibe outros organogramas que compartilham o mesmo tipo de entidade pai. Por exemplo, se você estiver visualizando um organograma de gerentes e funcionários (a entidade pai é usuário) e clicar nesse ícone, a lista de organogramas que podem ser exibidos só conterão relacionamentos em que a entidade pai também é usuário. Esse link interno pode ser configurado nas preferências de layout de organograma descritas em “Preferências de layout de organograma” na página 269
	Inicia uma ferramenta de e-mail para: ◆ Enviar os detalhes de identidade do usuário selecionado ◆ Compor um e-mail Esse link interno pode ser configurado nas preferências de layout de organograma descritas em “Preferências de layout de organograma” na página 269
	O link de pesquisa permite que os usuários pesquisem entidades. O resultado das pesquisas na entidade encontrada passa a ser o nó superior do gráfico exibido.
	Permite que os usuários detalhem até o nível seguinte.

Para obter mais informações sobre como adicionar e restringir os links internos nos organogramas, consulte “Preferências de layout de organograma” na página 269.

18.1.1 Sobre Relacionamentos de Organograma

O portlet Organograma exibe relacionamentos que são definidos na camada de abstração do diretório. Os relacionamentos a seguir ficam disponíveis depois que o aplicativo de usuário do Identity Manager é instalado.

- Participação no grupo
- Gerentes e Funcionários
- Grupos de Usuários

Para saber mais sobre como criar ou modificar relacionamentos de organograma, consulte o Capítulo 4, “Configurando a Camada de Abstração do Diretório” na página 75.

Observação: Grupos dinâmicos não têm suporte integral do portlet Organograma. Não é possível definir um grupo dinâmico como a entidade pai de um relacionamento, mas você pode definir um grupo dinâmico como a entidade filho de um relacionamento.

18.1.2 Sobre a exibição de Organograma

Por padrão, o organograma é exibido no frame do portlet, em uma área definida pelas preferências Largura do Portlet e Altura do Portlet. Se o conteúdo precisar de mais espaço do que a área definida, os limites do portlet se expandirão e a altura e a largura da página também. Para obter uma exibição integral do organograma, os usuários clicam no ícone de maximizar disponível na barra de título do portlet. (O organograma é exibido em modo de maximização total, por padrão, quando iniciado no porlet Detalhes.)

Imagens do usuário Por padrão, o layout do organograma para o Objeto do usuário inclui o atributo Fotografia do Usuário. Entretanto, se o cofre de identidade não incluir esse atributo ou se ele não for preenchido, o organograma ignorará esse atributo em tempo de execução. Se você armazenar suas fotografias em outro local, poderá configurar o organograma para exibi-las.

Para obter mais informações, consulte o Seção 18.2.3, “Carregando imagens dinamicamente” na página 274.

18.2 Configurando o portlet Organograma

Para configurar o portlet Organograma, você precisará:

Etapa	Tarefa	Descrição
1	Definir o relacionamento que você deseja exibir	Você pode usar um dos relacionamentos predefinidos que são instalados com o aplicativo de usuário do Identity Manager ou criar os seus próprios relacionamentos. Para obter mais informações sobre como definir um relacionamento, consulte o Capítulo 4, “Configurando a Camada de Abstração do Diretório” na página 75.
2	Verificar se as entidades e os atributos a serem usados no relacionamento estão disponíveis na camada de abstração do diretório	Para obter mais informações sobre como definir um relacionamento, consulte a Seção 18.2.1, “Configuração da camada de abstração do diretório” na página 264.
3	Determinar onde exibir esse relacionamento	Deseja criar uma nova página para iniciar o organograma? Ou deseja iniciá-lo no portlet Detalhes ou em outro organograma? Para obter mais informações sobre como criar páginas e adicionar portlet a essas páginas, consulte o Capítulo 7, “Administração de Página” na página 137.

Etapa	Tarefa	Descrição
4	Definir preferências para o portlet	As preferências permitem definir: ◆ Os atributos a serem exibidos ◆ Como exibi-las (seu layout HTML) Para obter mais informações, consulte a Seção 18.2.2, "Definindo preferências de organograma" na página 264.
5	Testar	Testar as definições e o layout do relacionamento
6	Definir os direitos do eDirectory e estabelecer os índices necessários para melhorar o desempenho	**Direitos efetivos** — Para exibir os atributos definidos pelo portlet, os usuários devem ter os direitos **Ler** aos atributos. **Aprimoramento do desempenho —** O desempenho da exibição do organograma pode ser melhorado com a inclusão do índice de valores do eDirectory no atributo filho do relacionamento, pois o atributo filho é usado para uma pesquisa LDAP.

18.2.1 Configuração da camada de abstração do diretório

As entidades e os atributos exibidos em um Organograma devem ser definidos na camada de abstração do diretório. A tabela a seguir mostra os atributos e as propriedades que devem ser definidas para cada entidade e atributo exibidos em um organograma.

Tipo de definição	Configuração	Valor
entidade	exibir	Selecionado (verdadeiro)
atributo	ler	Selecionado (verdadeiro)
	Pesquisar	Selecionado (verdadeiro)

Requisitos do link de pesquisa O link de pesquisa permite que os usuários naveguem pelo organograma procurando outros objetos do mesmo tipo da Chave de Entidade Pai. É preciso que a chave de entidade pai tenha ao menos um atributo com as propriedades de acesso *require* e *search* definidas como verdadeiras (selecionadas no editor da camada de abstração do diretório). Caso contrário, a caixa de diálogo Pesquisa de Objeto do link de pesquisa não poderá ser preenchida e permanecerá vazia.

Para obter mais informações sobre a configuração de entidades e atributos, consulte o Capítulo 4, "Configurando a Camada de Abstração do Diretório" na página 75.

18.2.2 Definindo preferências de organograma

Você define dois tipos de preferências:

- "Preferências de relacionamento de organograma" na página 265
- "Preferências de layout de organograma" na página 269

Preferências de relacionamento de organograma

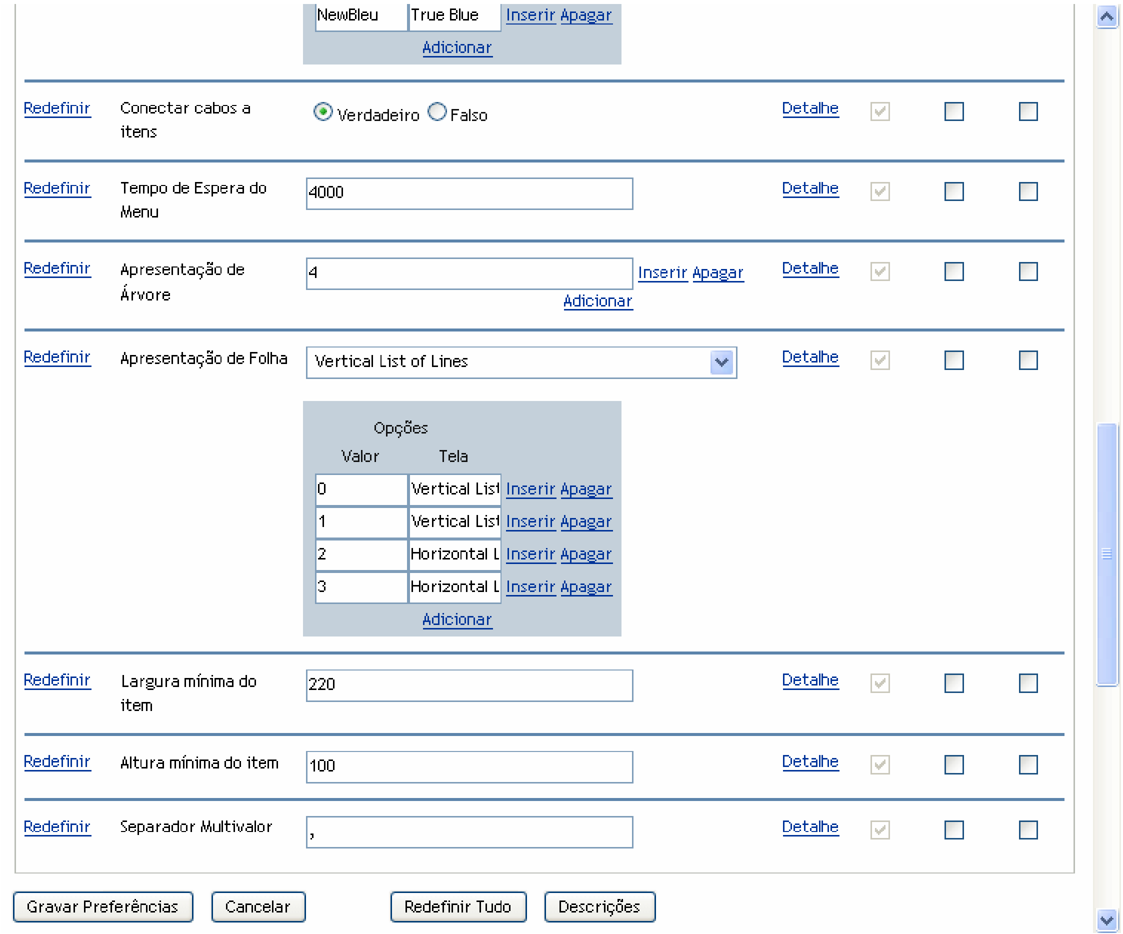
As preferências de relacionamento de organograma estão contidas em uma página de preferências.



.

.

.



Preferência	O que fazer
Layouts de Apresentação	Clique em Exibir/Edit Custom Preferences para acessar as preferências de layout. Elas estão descritas em “Preferências de layout de organograma” na página 269.
Chave de Relacionamento	Digite a chave de relacionamento. Esse valor deve corresponder a uma das chaves de relacionamento especificadas na camada de abstração do diretório.

Preferência	O que fazer

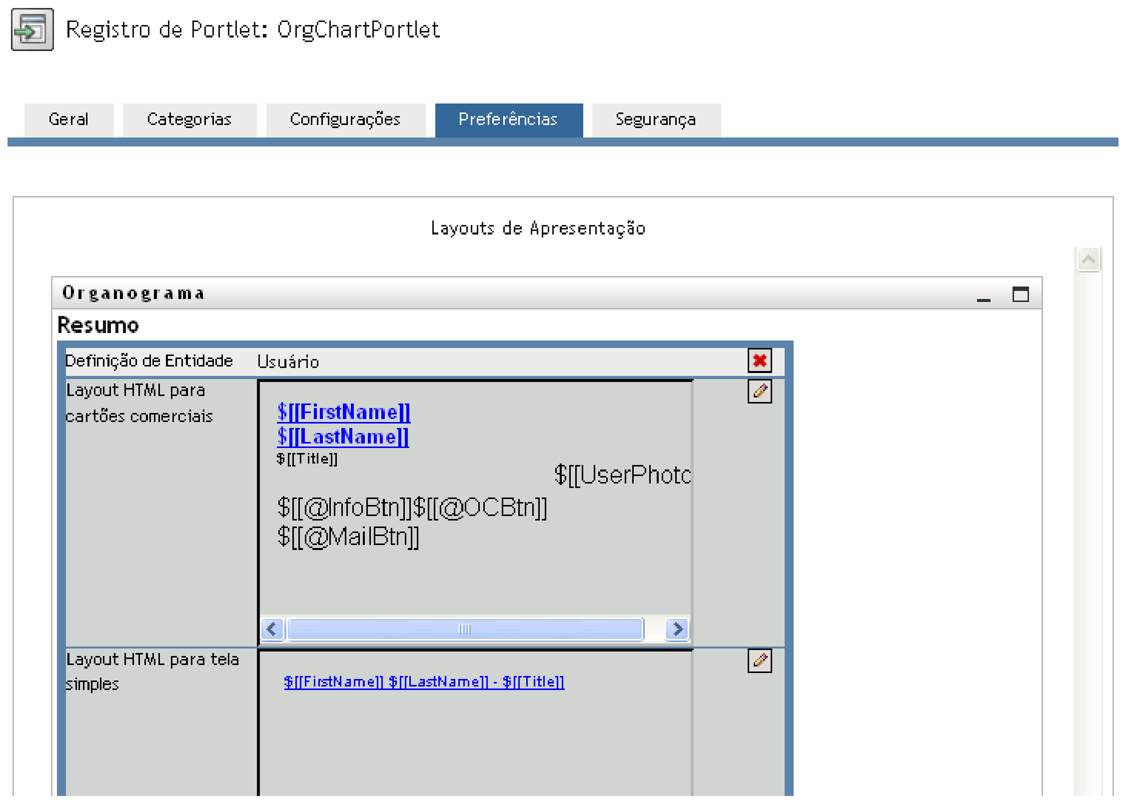
Chave de Entidade Pai	Digite o DN da entidade que representa o nó da raiz do organograma a ser exibido, ou, para exibir o organograma do usuário, digite ${User/id}. (O parâmetro ${User/id} é resolvido no DN do usuário.)
	
	Esse valor deve estar dentro dos nós especificados pela propriedade da raiz de pesquisa na camada de abstração do diretório ou a pesquisa LDAP falhará.
	
	Estes são alguns exemplos de DNs válidos (usando amostra de dados):
	
	◆ Para exibir a Chave de Relacionamento user2users com o funcionário chamado Jack Miller como a raiz do organograma, você especifica:
	
	`cn=jmiller,ou=users,ou=sample,o=novell`
	
	◆ Para exibir a Chave de Relacionamento group2users com o grupo Contabilidade como o nó da raiz, você especifica:
	
	`cn=Accounting,ou=groups,ou=sample,o=novell`

Profundidade padrão	Especifica a profundidade do organograma quando ele é exibido pela primeira vez. ◆ 0 — Mostrar somente a raiz ◆ 1 — Mostrar a raiz e seus filhos ◆ 2 — Mostrar a raiz, seus filhos e netos e assim por diante. Se esse valor receber um incremento e ficar superior à Profundidade Máxima (abaixo), o valor da profundidade máxima terá precedência.
Profundidade Máxima	Define a profundidade máxima de detalhamento em um organograma. É como navegar em um organograma limitado por direitos efetivos.
Máscara de Organograma	Cartão Comercial eGuide Novell.com Conectado True Blue
Conectar cabos a itens	Especifica se os curingas do organograma são conectados por cabos. Falso indica não conectado.
Menu Tempo de Espera	Número de milissegundos antes do menu (para os links internos) em exibição desaparecer.

Preferência	O que fazer
Apresentação de Árvore	Define a orientação, a distribuição e a aparência por nível de profundidade do organograma. Os *n* primeiros valores definirão orientação, distribuição e aparência dos níveis de 0 a *n-1*. O último valor será usado repetidamente para níveis de profundidade superiores a *n-1*. Os valores devem estar entre 0 e 5. Os valores são: 0: Coloca o curinga acima de uma lista vertical de itens 1: Linha acima de uma lista vertical de itens 2: Coloca o curinga acima de uma lista horizontal de itens 3: Linha acima de uma lista horizontal de itens 4: Coloca o curinga acima de uma lista horizontal de itens 5: Linha antes de uma lista vertical de itens
Apresentação de Folha	Define a orientação, a distribuição e a aparência para a maior profundidade de uma ramificação do organograma.
Largura mínima do item	Este valor deve ser igual ao valor arredondado ('altura mínima do item' * 1.618)
Altura mínima do item	Este valor deve ser igual ao valor arredondado ('largura mínima do item' / 1.618)
Separador para atributos multivalor	O caractere utilizado como um separador para atributos com mais de um valor.

Preferências de layout de organograma

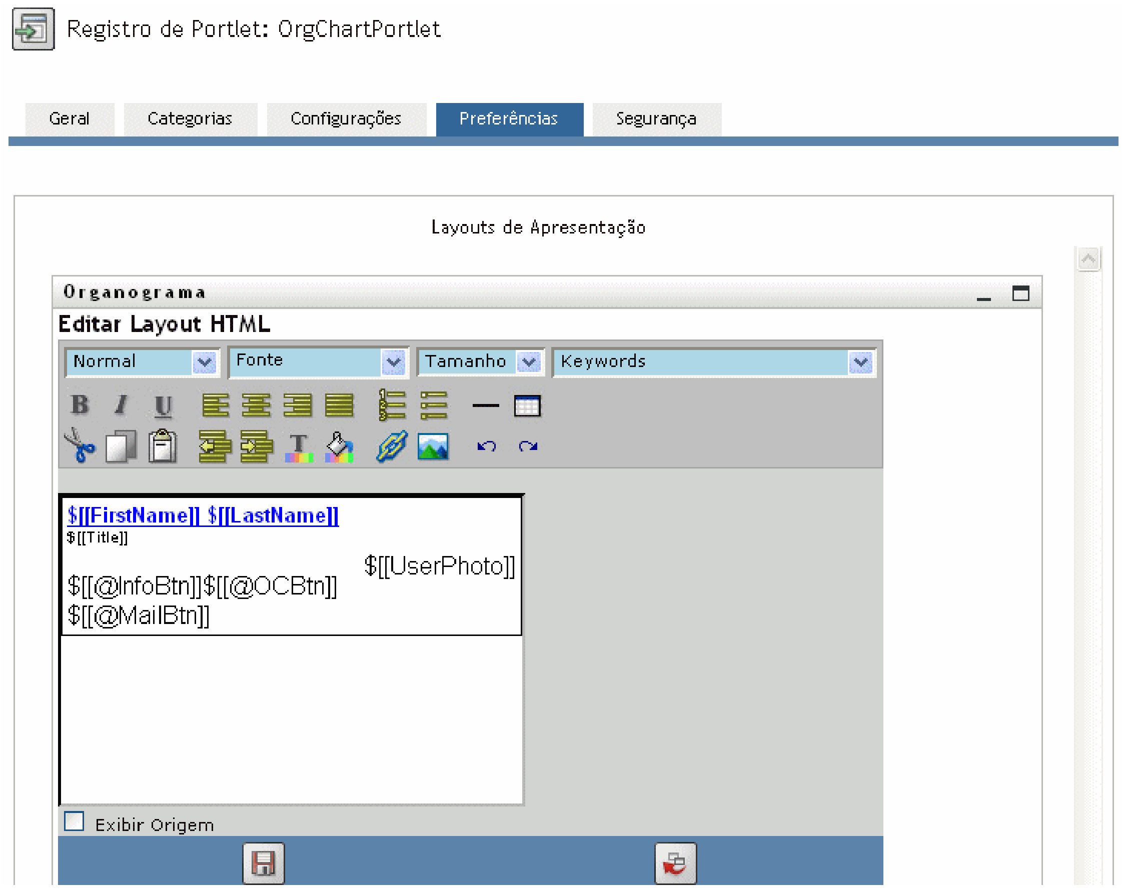
As preferências de layout de organograma permitem que você defina o layout HTML para a exibição de entradas do organograma. Você pode usar o editor de HTML de sua escolha para uma edição mais precisa. Consulte "Para usar um editor externo" na página 274.)



Layout HTML para cartões comerciais — O layout padrão.

Layout HTML para tela simples — O layout exibido quando a preferência da apresentação de árvore está definida como 1.

Editor de HTML Para acessar o editor de HTML, você clica no botão editar. Assim é o editor de HTML:



Usando o Editor de HTML

O Editor de HTML tem uma interface cuja aparência visual é compatível com os resultados e que permite definir o layout das folhas do organograma. Ele tem os recursos típicos de um editor de HTML para definir a formatação do texto e das listas, e também especificar âncoras e imagens, entre outros. Use a lista suspensa *Palavras-chave* para posicionar atributos, comandos e URLs de navegação na área de layout. Quando você escolhe uma palavra-chave na lista suspensa, ela é inserida com a sintaxe apropriada, mas você também pode adicionar HTML na área de layout.

Palavras-chave Ao criar seu layout, você pode usar a lista suspensa Palavras-chave para inserir variáveis que serão substituídas em tempo de execução por valores de atributo específicos. Você também pode digitar as referências usando esta sintaxe:

```
$[[palavra-chave]]
```

Onde *palavra-chave* é o valor de um atributo de entidade como LastName.

Você pode concatenar atributos usando esta sintaxe:

```
$[[palavra-chave+palavra-chave]]
```

Por exemplo:

```
$[[FirstName+LastName]]
```

Você pode concatenar quantos atributos quiser e também incluir strings entre aspas como esta:

```
$[[palavra-chave+”exemplo de texto”+palavra-chave]]
```

Os valores das palavras-chave e do texto entre aspas serão renderizados.

Observação: Palavras-chave com erros ortográficos no layout serão processadas com tais erros no organograma (incluindo $[[]]).

Recursos do Editor de HTML e o uso de palavras-chave Para usar recursos do Editor de HTML e a lista suspensa Palavras-chave:

Recurso	Dica
Botão Inserir Link	Para inserir um link: **No Mozilla:** 1. Realce o texto do hiperlink e clique em **Inserir Link**. 2. Digite o URL e clique em **Criar Link**. 3. Grave as preferências. **No IE:** 1. Clique em Inserir Link. 2. Digite o URL na janela popup. 3. Realce o texto do hiperlink e clique em **Criar Link** (na janela popup). 4. Grave as preferências. **Observação:** Se a imagem ou o URL estiver no quadrante superior esquerdo do Editor de HTML, a janela popup o sobreporá. Como a janela popup não pode ser movida, você terá que criar o texto em outra parte do editor, e depois cortá-lo e colá-lo no local correto.

<table>
<tr><th>Recurso</th><th>Dica</th></tr>
<tr><td>Botão Adicionar Imagem</td><td>No Mozilla:
1. Posicione o mouse onde você deseja inserir uma imagem e clique em Adicionar Imagem.
2. Digite o URL e o texto e clique em Criar Imagem na janela popup.
3. Grave as preferências.
No IE:
1. Clique em Adicionar Imagem.
2. Digite o URL e o texto na janela popup e posicione o mouse onde deseja inserir uma imagem. Em seguida, clique em Criar Imagem na janela popup.
3. Grave as preferências.
Observação: Se a imagem ou o URL estiver no quadrante superior esquerdo do Editor de HTML, a janela popup o sobreporá. Como a janela popup não pode ser movida, você terá que criar o texto em outra parte do editor, e depois cortá-lo e colá-lo no local correto.</td></tr>
<tr><td>Lista suspensa Palavra-chave: Atributos</td><td>É o conjunto de atributos que estão disponíveis para a entidade.</td></tr>
<tr><td>Lista suspensa Palavra-chave: Comandos</td><td>Estes comandos permitem que o portlet Organograma iniciem outros portlets de identidade ou recursos internos como as ferramentas de IM ou e-mail.
◆ Botão Ação do IM — Cria um botão para o envio de mensagens instantâneas
◆ Botão Ação do Correio — Cria um botão para o envio de e-mails
◆ Botão Ação do OrgChart — Cria um botão para alternar para outro relacionamento, com a instância de entidade selecionada como o pai
◆ Botão Ação de Informações — Inicia o portlet Detalhes
Para obter exemplos dos botões que são gerados, consulte “Links internos” na página 262.</td></tr>
</table>

Recurso	Dica
URLs	**Link URL de Navegação de Organograma** — Permite que você especifique um atributo de URL ou de entidade que será exibido como um link. Quando o usuário clicar no link, o portlet Organograma será reexibido com a entidade clicada como o nó da raiz.

Restrição:

Isso só é válido quando as entidades pai e filho de um relacionamento são do mesmo tipo de objeto. Por exemplo, no relacionamento entre Gerentes e Funcionários, os dois são usuários.

Dicas de uso:

Para usar esta palavra-chave, é preciso:

1. Clique em Exibir Origem.
2. Digite a palavra-chave @NavUrl usando esta sintaxe:

```
<a href="javascript:$[[@NavUrl]]">Texto</a>
```

onde *Texto* é o link a ser exibido em tempo de execução ou um atributo de entidade. No exemplo a seguir, **Clique aqui** é um link em que é possível clicar.

```
<a href="javascript:$[[@NavUrl]]">Clique aqui</a>
```

No exemplo, o atributo FirstName é um link em que é possível clicar:

```
<a href="javascript:$[[@NavUrl]]">$[[FirstName]]</
a>
```

Restrição de uso:

Com o Internet Explorer, você **não pode** usar a sintaxe a seguir.

```
<a href="$[[@NavUrl]]">someText</a>
```

Durante uma operação de gravação, o Internet Explorer adiciona:

```
http://context before $[[@NavUrl]]
```

Isso significa que

```
<a href="$[[@NavUrl]]">someText</a>
```

se torna

```
<a href="http://localhost/.../
$[[@NavUrl]]">someText</a>
```

Recurso	Dica
	Link Clique de Navegação de Organograma — Use esta palavra-chave para um evento onClick. (Permite que somente a área do portlet de organograma seja atualizada, e não a página inteira.) **Dicas de uso:** Para usar esta palavra-chave, é preciso: 1. Clicar em Exibir Origem. 2. Digitar a palavra-chave @NavClick usando esta sintaxe: `<A href="javascript:return false;" onClick="$[[@NavClick]]">$[[`*`Atributo`*`]]</A>` onde *Atributo* é um atributo de entidade que se torna um link em que é possível clicar. "javascript:return false;" é obrigatório. Sua omissão causará um erro.

Para gravar os layouts definidos, clique em *Submeter*.

Para usar um editor externo Você pode usar um editor externo de HTML:

1. Criando a origem HTML dos atributos de entidade, comandos e palavras-chave com o Editor de Layout HTML disponível nas preferências.
2. Copiando a origem HTML para o editor de sua escolha.
3. Fazendo as mudanças desejadas.
4. Copiando a origem HTML de volta para a preferência do Editor de Layout HTML depois de editá-la.

18.2.3 Carregando imagens dinamicamente

Para exibir imagens, como fotografias do usuário, que estão armazenadas no cofre de identidade, é possível adicionar o nome do atributo ao cartão comercial. Por exemplo, a inclusão do atributo Fotografia do Usuário ao layout do cartão comercial exibe a foto do usuário.

Se você armazena imagens fora do cofre de identidade, precisará usar a tag IMG: no *modo Exibir Origem* do Editor de HTML da seguinte maneira:

1. Vá até as preferências do portlet Organograma e acesse o Editor de HTML.
2. Clique em *Exibir Origem*.
3. Use a tag IMG: para combinar um local, uma chave de atributo e uma extensão de arquivo usando uma sintaxe como esta:

```
$[[IMG:”URL” + atributo-chave-nome + ”fileextension”]]
```

O exemplo a seguir mostra a sintaxe usada caso você tenha armazenado fotografias dos funcionários como imagens JPG de acordo com Sobrenome no subdiretório /images do servidor de aplicativos:

```
$[[IMG:"http://myhost:8080/images/"+LastName+".jpg"]]
```

Em tempo de execução, o organograma concatena o URL com o atributo LastName e a extensão de arquivo .jpg.

Lembre-se de que o Editor de HTML oferece suporte a uma sintaxe flexível. Ele aceita qualquer combinação de texto e atributos de forma que se obtenha uma sintaxe como:

```
$[[IMG:”qualquer texto” + atributo-chave-nome + ...]]
```

Referência dos portlets Gerenciamento de Senhas 19

Este capítulo ensina a adicionar recursos de auto-atendimento de senha e autenticação do usuário ao aplicativo de usuário do Identity Manager. Os tópicos incluem:

19.1 Preparando o gerenciamento de senhas

Para preparar-se para dar suporte ao auto-atendimento de senha e à autenticação do usuário no aplicativo de usuário do Identity Manager, é importante ter as seguintes informações:

19.1.1 Sobre os recursos de gerenciamento de senhas

Os recursos de gerenciamento de senhas suportados por um aplicativo de usuário do Identity Manager abrangem a *autenticação do usuário* e o *auto-atendimento de senha*. Quando usados, os recursos permitem ao aplicativo:

- Solicitar informações de *login* (nome de usuário e senha) para autenticação no Novell eDirectory
- Oferecer aos usuários auto-atendimento para a *mudança de senha*
- Oferecer aos usuários auto-atendimento de *senha esquecida* (incluindo solicitação de respostas de verificação e exibição de dica de senha, ou permitindo uma mudança de senha, caso seja necessário)
- Fornecer aos usuários auto-atendimento de *pergunta de verificação*
- Oferecer aos usuários auto-atendimento de *dica de senha*

19.1.2 Configuração necessária no eDirectory

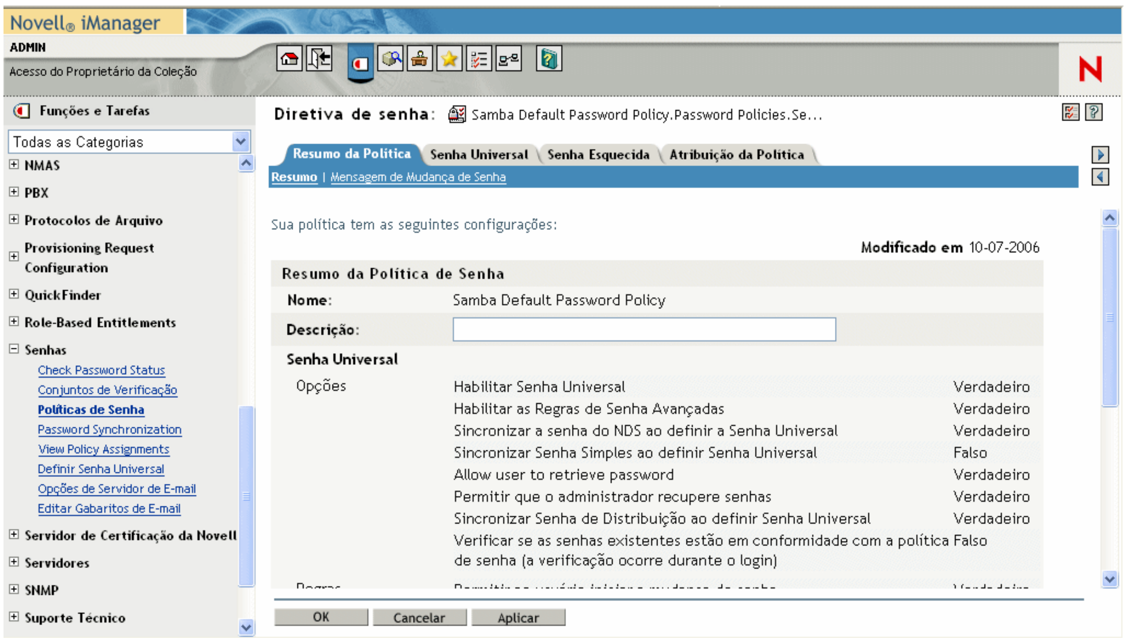
Antes de usar a maioria dos recursos de auto-atendimento de senha e autenticação do usuário, é preciso fazer o seguinte no eDirectory:

- Habilitar *Senha Universal*
- Criar uma ou mais *políticas de senha*

- Atribuir as políticas de senha apropriadas aos *usuários*

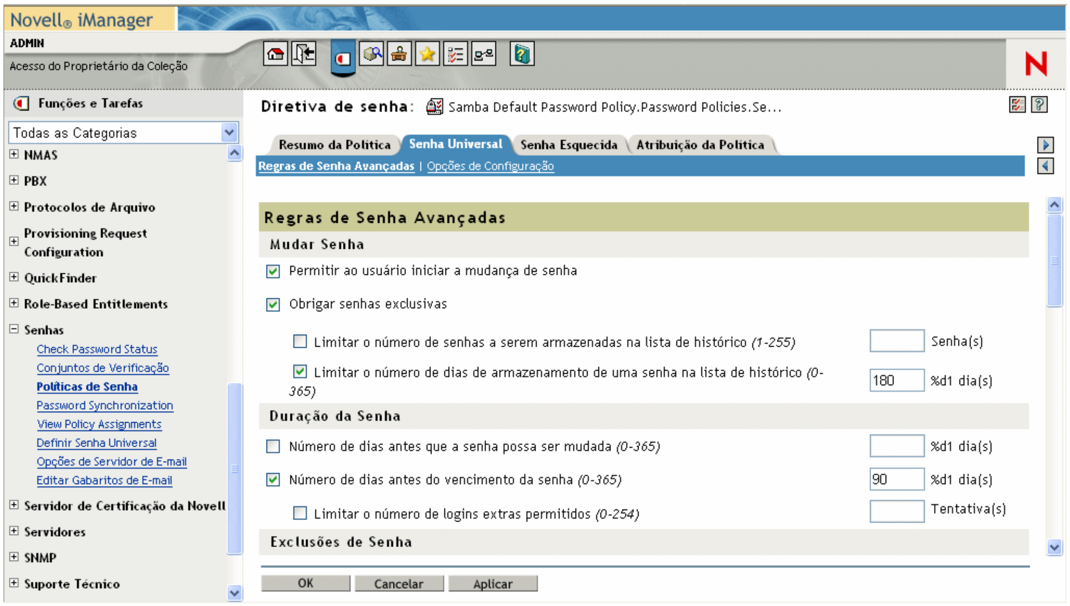
Uma política de senha é um conjunto de regras definidas pelo administrador que especificam os critérios para a criação e a substituição de senhas do usuário. O Novell Identity Manager aproveita o *NMAS* (Novell Modular Authentication Service) para assegurar o uso das políticas de senha atribuídas aos usuários no eDirectory.

Você pode usar o *Novell iManager* para executar as etapas de configuração necessárias. Por exemplo, veja aqui como alguém definiu a Política DocumentationPassword no iManager.

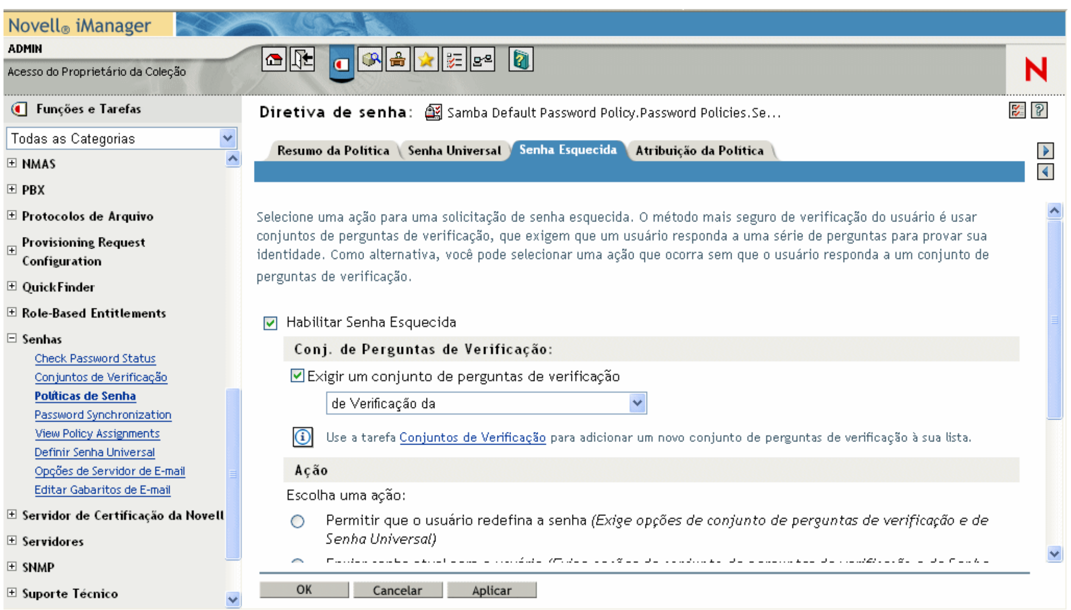


Essa política de senha especifica:

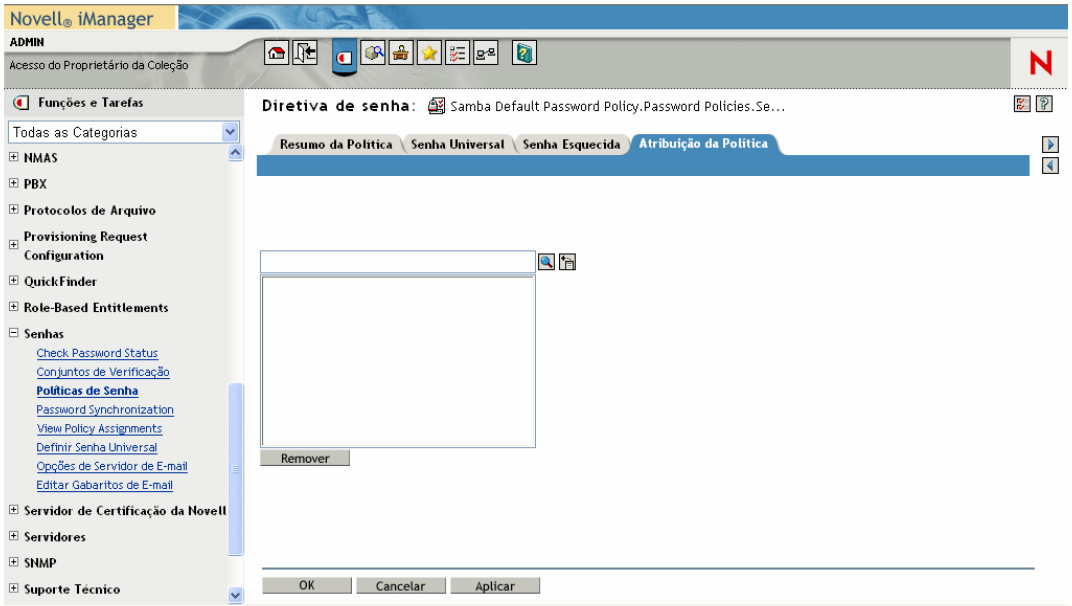
- Configurações de *Senha Universal*



- Configurações para tratar de situações com *senha esquecida*



- *Atribuições* que aplicam a política a usuários específicos



Para obter mais informações sobre como configurar Senha Universal e políticas de senha no eDirectory, consulte o Guia de Administração do Novell Identity Manager (http://www.novell.com/documentation/dirxml20/index.html).

19.2 Sobre os portlets de senha

Para implementar recursos de auto-atendimento de senha e autenticação do usuário no aplicativo de usuário do Identity Manager, você usará os seguintes portlets:

Portlet	Descrição
Seção 19.3, "Portlet Login do IDM" na página 282	O Login do IDM oferece autenticação robusta do usuário com suporte no Identity Manager (por meio de Senha Universal, políticas e senha e o NMAS). O portlet Login do IDM é redirecionado para os outros portlets de senha conforme o necessário durante o processo de login.
Seção 19.4, "Portlet Resposta de Verificação do IDM" na página 283	Este portlet de auto-atendimento permite aos usuários: • Configurar respostas válidas às perguntas de verificação definidas pelo administrador e configurar perguntas e respostas de verificação definidas pelo usuário • Mudar as respostas válidas às perguntas de verificação definidas pelo administrador e mudar as perguntas e as respostas de verificação definidas pelo usuário
Seção 19.5, "Portlet Definição de Dica do IDM" na página 285	Este portlet de auto-atendimento permite que os usuários configurem ou mudem sua dica de senha (que pode ser exibida ou enviada por e-mail como dica em situações de senha esquecida).

Portlet	Descrição
Seção 19.6, “Portlet Mudar Senha do IDM” na página 286	Este portlet de auto-atendimento permite que os usuários mudem (redefinam) sua Senha Universal, de acordo com a política de senha esquecida atribuída. Ele usa essa política para exibir as regras a que a nova senha deve obedecer. Se a Senha Universal não estiver habilitada, o portlet mudará a senha do eDirectory (simples) do usuário, como permitido nas Restrições de Senha do usuário.
Seção 19.7, “Portlet Senha Esquecida do IDM” na página 287	Este portlet de auto-atendimento usa a autenticação de resposta de verificação para que o usuário possa obter informações sobre sua senha (no NMAS). O resultado, que depende da política de senha atribuída, pode incluir: ◆ Exibição da dica de senha do usuário na tela ◆ Envio da dica ao usuário por e-mail ◆ Envio da senha ao usuário por e-mail ◆ Solicitação para que o usuário redefina (mude) a senha

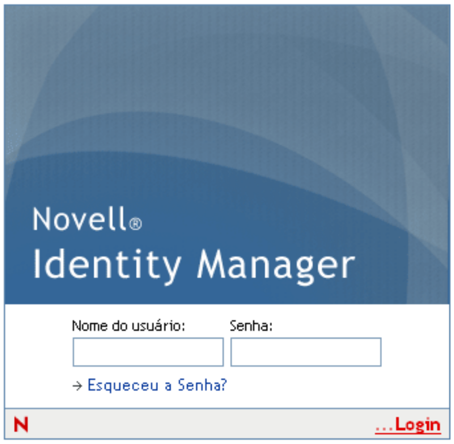
19.2.1 Modos do portlet de auto-atendimento de senha

Os portlets de auto-atendimento de senha (Resposta de Verificação do IDM, Definição de Dica do IDM e Mudar Senha do IDM) operam em dois modos:

Modo	Descrição	Comportamento em tempo de execução
Modo independente	Os portlets são executados de forma independente em páginas compartilhadas.	◆ Se o portlet for executado **corretamente**, ele exibirá uma mensagem de sucesso com um link para reexecução da operação. ◆ Se o portlet for **malsucedido**, ele exibirá uma mensagem de erro no formulário.
Modo de delegação	Os portlets são exibidos em uma página como resultado de uma verificação de validação durante o login.	◆ Se o portlet for executado **corretamente**, o usuário será redirecionado a um novo portlet ou à página principal do aplicativo de usuário. Nenhuma mensagem de êxito é exibida. ◆ Se o portlet for **malsucedido**, ele exibirá uma mensagem de erro no formulário.

19.3 Portlet Login do IDM

O portlet Login do IDM realiza uma autenticação robusta do usuário com suporte no Identity Manager (por meio de Senha Universal, políticas e senha e o NMAS). O portlet Login do IDM é redirecionado para os outros portlets de senha conforme o necessário durante o processo de login.



19.3.1 Requisitos

O Login do IDM apresenta os seguintes requisitos:

Tópico	Requisitos
Política de senha	Este portlet não requer uma política de senha, a não ser que você queira usar regras avançadas ou permitir que os usuários cliquem no link **Senha Esquecida**.
Senha Universal	Este portlet não requer que a Senha Universal seja habilitada, a não ser que você queira usar uma política de senha com regras avançadas.
SSL	Este portlet usa SSL; portanto, verifique se o servidor de aplicativos está configurado corretamente para dar suporte a conexões SSL com o domínio LDAP.

19.3.2 Uso

Para usar o portlet Login do IDM, você precisa informar-se sobre o seguinte:

- "Como o Login do IDM é redirecionado para outros portlets" na página 282
- "Usando logins extras" na página 283

Como o Login do IDM é redirecionado para outros portlets

Em tempo de execução, o portlet Login do IDM é redirecionado para outros portlets de senha conforme o necessário para concluir o processo de login. Por exemplo:

Se o usuário	O Login do IDM é redirecionado para
Clica no link **Senha Esquecida**	Seção 19.7, "Portlet Senha Esquecida do IDM" na página 287
Precisa configurar perguntas e respostas de verificação	Seção 19.4, "Portlet Resposta de Verificação do IDM" na página 283
Precisa configurar sua dica de senha	Seção 19.5, "Portlet Definição de Dica do IDM" na página 285
Precisa redefinir uma senha inválida	Seção 19.6, "Portlet Mudar Senha do IDM" na página 286

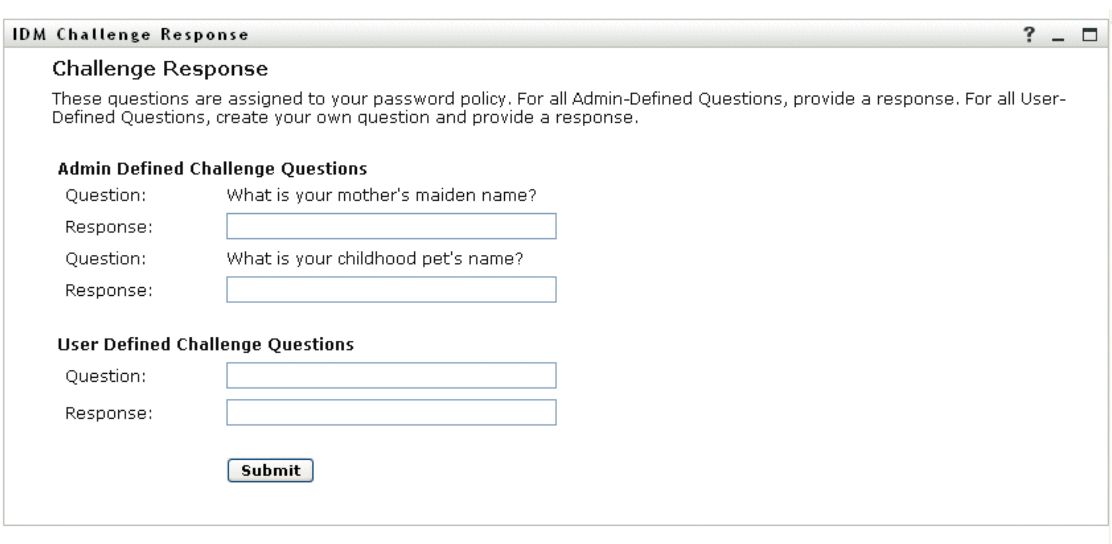
Usando logins extras

Se você usar um login extra, o portlet Login do IDM exibirá uma mensagem de aviso que lhe pede para mudar sua senha e indica o número de logins extras restantes. Caso você esteja em seu último login, o portlet Login do IDM o redirecionará para o portlet Mudar Senha do IDM.

19.4 Portlet Resposta de Verificação do IDM

Este portlet de auto-atendimento permite aos usuários:

- Configurar respostas válidas às perguntas de verificação definidas pelo administrador e configurar perguntas e respostas de verificação definidas pelo usuário
- Mudar as respostas válidas às perguntas de verificação definidas pelo administrador e mudar as perguntas e as respostas de verificação definidas pelo usuário



19.4.1 Requisitos

O portlet Resposta de Verificação do IDM apresenta os seguintes requisitos:

Tópico	Requisitos
Política de senha	Este portlet requer uma política de senha com o recurso de senha esquecida habilitado e um conjunto de verificações.
Senha Universal	Este portlet não requer que a Senha Universal seja habilitada.
Configuração do eDirectory	Este portlet requer direitos de supervisor para o Administrador de Aplicativo de Usuário no container em que o usuário conectado reside. A concessão desses privilégios permite que o usuário grave uma resposta de verificação para o armazenamento secreto. Por exemplo, suponha que o administrador de domínio LDAP seja cn=admin, ou=sample, n=novell e que você efetue login como cn=user1, ou=testou, o=novell. Você precisa atribuir cn=admin, ou=sample, n=novell como um trustee de **testou**, e conceder direitos de supervisor em **[Todos os direitos de atributos]**.

19.4.2 Uso

Para usar o portlet Resposta de Verificação do IDM, você precisa informar-se sobre o seguinte:

- "Como a Resposta de Verificação do IDM é usada durante o login" na página 284
- "Como a Resposta de Verificação do IDM é usada no aplicativo de usuário" na página 284

Como a Resposta de Verificação do IDM é usada durante o login

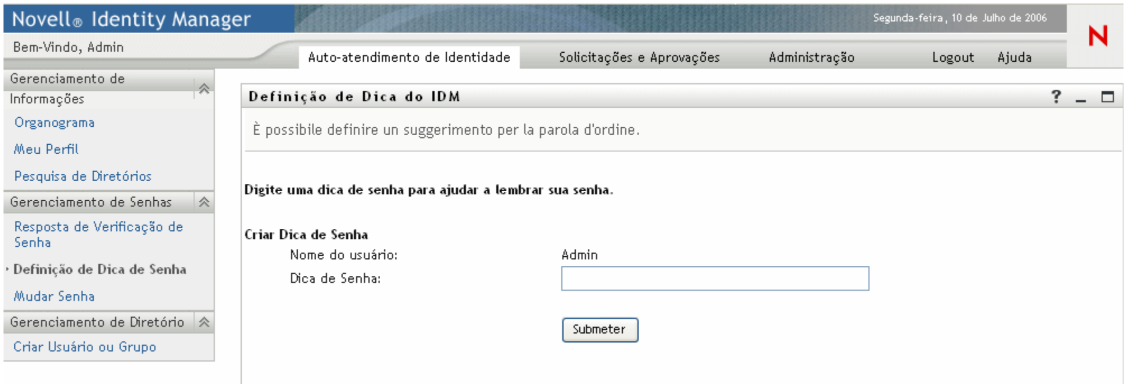
Durante o processo de login, o Portlet Login do IDM (página 282) é redirecionado automaticamente para o portlet Resposta de Verificação do IDM sempre que o usuário precisa configurar perguntas e respostas de verificação (por exemplo, a primeira vez que o usuário tenta efetuar login no aplicativo depois que o administrador atribui ao usuário uma política de senha no iManager. A política de senha deve ter o recurso de senha esquecida habilitado e incluir um conjunto de verificações).

Como a Resposta de Verificação do IDM é usada no aplicativo de usuário

Por padrão, o aplicativo de usuário oferece serviço de auto-atendimento para mudar perguntas e respostas de verificação.

19.5 Portlet Definição de Dica do IDM

Este portlet de auto-atendimento permite que os usuários configurem ou mudem sua dica de senha (que pode ser exibida ou enviada por e-mail como dica em situações de senha esquecida).



19.5.1 Requisitos

O portlet Definição de Dica do IDM apresenta os seguintes requisitos:

Tópico	Requisitos
Política de senha	Este portlet requer uma política de senha com o recurso de senha esquecida habilitado e um conjunto de verificações.
Senha Universal	Este portlet não requer que a Senha Universal seja habilitada.

19.5.2 Uso

Para usar o portlet Definição de Dica do IDM, você precisa informar-se sobre o seguinte:

- "Como a Definição de Dica do IDM é usada durante o login" na página 285
- "Usando a Definição de Dica do IDM na página do aplicativo de usuário" na página 285

Como a Definição de Dica do IDM é usada durante o login

Durante o processo de login, o Portlet Login do IDM (página 282) é redirecionado automaticamente para o portlet Definição de Dica do IDM sempre que o usuário precisa configurar sua dica de senha (por exemplo, a primeira vez que o usuário tenta efetuar login no aplicativo depois que o administrador atribui ao usuário uma política de senha no iManager. A política de senha terá o recurso de senha esquecida habilitado e a ação definida como *Enviar dica por e-mail* ou *Mostrar dica na página*).

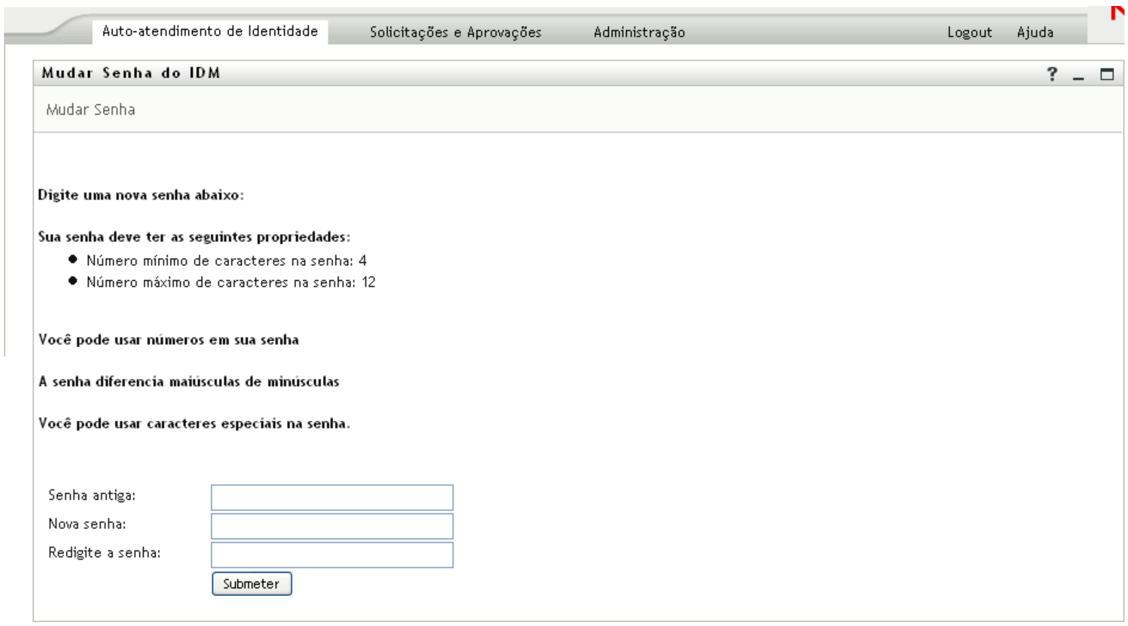
Usando a Definição de Dica do IDM na página do aplicativo de usuário

Por padrão, o aplicativo de usuário oferece serviço de auto-atendimento para mudar perguntas e respostas de verificação.

19.6 Portlet Mudar Senha do IDM

Este portlet de auto-atendimento permite que os usuários mudem (redefinam) sua Senha Universal, de acordo com a política de senha esquecida atribuída. Ele usa essa política para exibir as regras a que a nova senha deve obedecer.

Se a Senha Universal não estiver habilitada, o portlet mudará a senha do eDirectory (simples) do usuário, como permitido nas Restrições de Senha do usuário.



19.6.1 Requisitos

O portlet Mudar Senha do IDM apresenta os seguintes requisitos:

Tópico	**Requisitos**
Configuração da camada de abstração do diretório	Nenhuma configuração da camada de abstração do diretório é necessária para este portlet.
Política de senha	Este portlet não requer que uma política de senha, a não ser que você queira usar regras de senha avançadas (com a Senha Universal habilitada).
Senha Universal	Para usar este portlet para uma Senha Universal, a configuração **Permitir que o usuário mude a senha** deve estar habilitada nas Regras de Senha Avançadas da política de senha do usuário atribuído. Para usar este portlet para uma senha do eDirectory (simples), a configuração **Permitir que usuário mude a senha** deve ser habilitada nas Restrições de Senha do usuário.

19.6.2 Uso

Para usar o portlet Mudar Senha do IDM, você precisa informar-se sobre o seguinte:

- "Como o portlet Mudar Senha do IDM é usado durante o login" na página 287
- "Usando o portlet Mudar Senha do IDM no aplicativo de usuário" na página 287

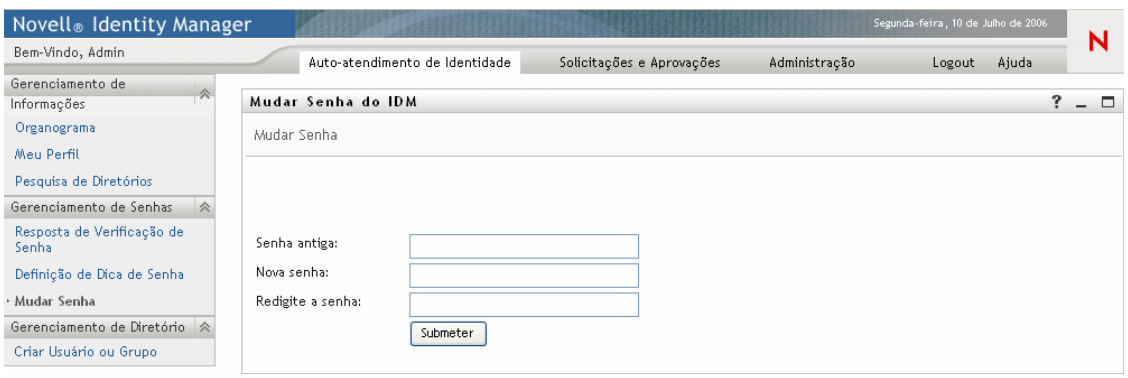
Como o portlet Mudar Senha do IDM é usado durante o login

Durante o processo de login, o Portlet Login do IDM (página 282) é redirecionado automaticamente para o portlet Mudar Senha do IDM sempre que o usuário precisa redefinir uma senha inválida (por exemplo, a primeira vez que o usuário tenta efetuar login em um aplicativo depois que o administrador implementa uma política de senha que exija a redefinição de suas senhas).

O Portlet Senha Esquecida do IDM (página 287) também é redirecionado automaticamente para o portlet Mudar Senha do IDM se a política de senha designada do usuário especificar que a senha deve ser redefinida quando for esquecida.

Usando o portlet Mudar Senha do IDM no aplicativo de usuário

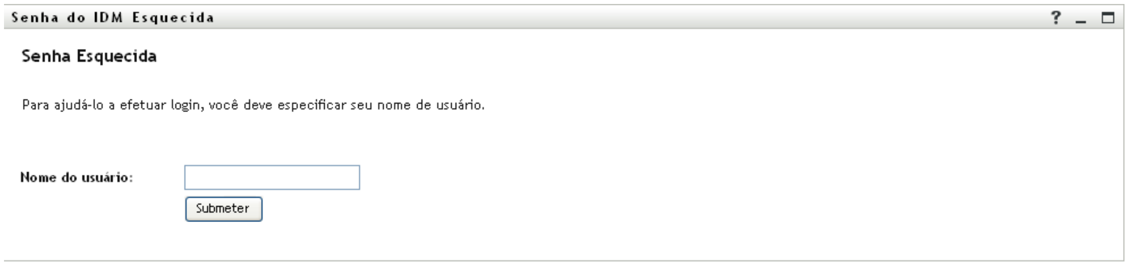
Por padrão, o aplicativo de usuário oferece serviço de auto-atendimento para mudar senhas usando o portlet Mudar Senha do IDM. Por exemplo:



19.7 Portlet Senha Esquecida do IDM

Este portlet de auto-atendimento usa a autenticação de resposta de verificação para que o usuário possa obter informações sobre sua senha. O resultado, que depende da política de senha atribuída, pode incluir:

- Exibição da dica de senha do usuário na tela
- Envio da dica ao usuário por e-mail
- Envio da senha ao usuário por e-mail
- Solicitação para que o usuário redefina (mude) a senha



19.7.1 Requisitos

O portlet Senha Esquecida do IDM apresenta os seguintes requisitos:

Tópico	Requisitos
Política de senha	Este portlet requer uma política de senha com o recurso de senha esquecida habilitado e um conjunto de verificações.
Senha Universal	Este portlet não requer que a Senha Universal seja habilitada (a não ser que você queira usar estas ações políticas de senha esquecida: redefinir senha ou enviar senha por e-mail ao usuário).

19.7.2 Uso

Para usar o portlet Senha Esquecida do IDM, você precisa informar-se sobre o seguinte:

- "Como o portlet Senha Esquecida do IDM é usado durante o login" na página 288
- "Configurando seu ambiente para ações de e-mail" na página 289
- "Preferências do portlet Senha Esquecida do IDM" na página 289

Como o portlet Senha Esquecida do IDM é usado durante o login

Durante o processo de login, o Portlet Login do IDM (página 282) é redirecionado para o portlet Senha Esquecida do IDM se o usuário clica no link *Senha Esquecida*. Estas são as ações do portlet Senha Esquecida do IDM quando exibido:

1. Solicita o *nome de usuário*.
2. É redirecionado para Portlet Login do IDM (página 282) para realizar a *autenticação de resposta de verificação* do usuário.
3. Executa a *ação de senha esquecida* especificada na política de senha designada do usuário autenticado. Ele segue um dos seguintes procedimentos:
   - *É redirecionado* para o Portlet Mudar Senha do IDM (página 286) para que o usuário possa redefinir sua senha
   - *Envia por email* a senha ou dica para o usuário
   - *Exibe* a dica

Observação: O portlet Senha Esquecida do IDM não se destina ao uso independente. Isso significa que você não deve planejar adicioná-lo a uma página compartilhada no aplicativo de usuário. A

inserção deste portlet em uma página cria um risco potencial de segurança de pessoas que mudam a senha em um computador automaticamente sem a permissão ou o conhecimento do usuário.

Configurando seu ambiente para ações de e-mail

Caso você queira aceitar ações de e-mail de senha esquecida, precisará saber se o *servidor de notificação por e-mail* está configurado corretamente:

1. Use um browser da Web para acessar o *iManager* no servidor do eDirectory e efetue login como *administrador*.
2. Vá para *Funções e Tarefas* > *Senhas* e selecione *Opções do Servidor de E-mail*.
3. Especifique as configurações apropriadas e clique em *OK*.

O portlet Senha Esquecida do IDM usa dois *gabaritos de e-mail*. No iManager, eles estão em *Funções e Tarefas>Senhas>Editar Gabaritos de E-mail*. Eles se chamam:

- Solicitação de dica de senha
- A solicitação de senha

Você pode mudar como quiser o conteúdo desses gabaritos para o seu aplicativo (só não pode mudar a estrutura).

Preferências do portlet Senha Esquecida do IDM

O portlet Senha Esquecida do IDM apresenta as seguintes preferências:

Preferência	Detalhes
login-sequence	A seqüência de login do NMAS a ser usada. Nesta versão, o portlet só tem suporte para **Resposta de Verificação**.
n4u.nds.ldap.ssl-port	A porta LDAP segura a ser usada. O padrão é **636**.
allow-wildcard	Indica se o usuário pode digitar curingas ao informar o nome de usuário. O padrão é **falso**.
encoding	A codificação de caracteres a ser usada. O padrão é **utf-8**.

Referência do portlet Lista de Pesquisa

20

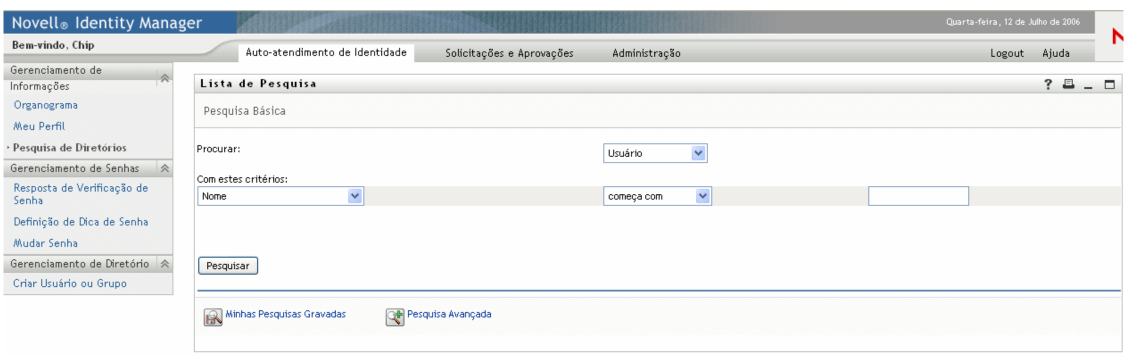
Este capítulo descreve como configurar e personalizar o portlet *Lista de Pesquisa* para ser usado com o aplicativo de usuário do Identity Manager. Os tópicos incluem:

- Seção 20.1, "Sobre a Lista de Pesquisa" na página 291
- Seção 20.2, "Configurando o portlet Lista de Pesquisa" na página 296

20.1 Sobre a Lista de Pesquisa

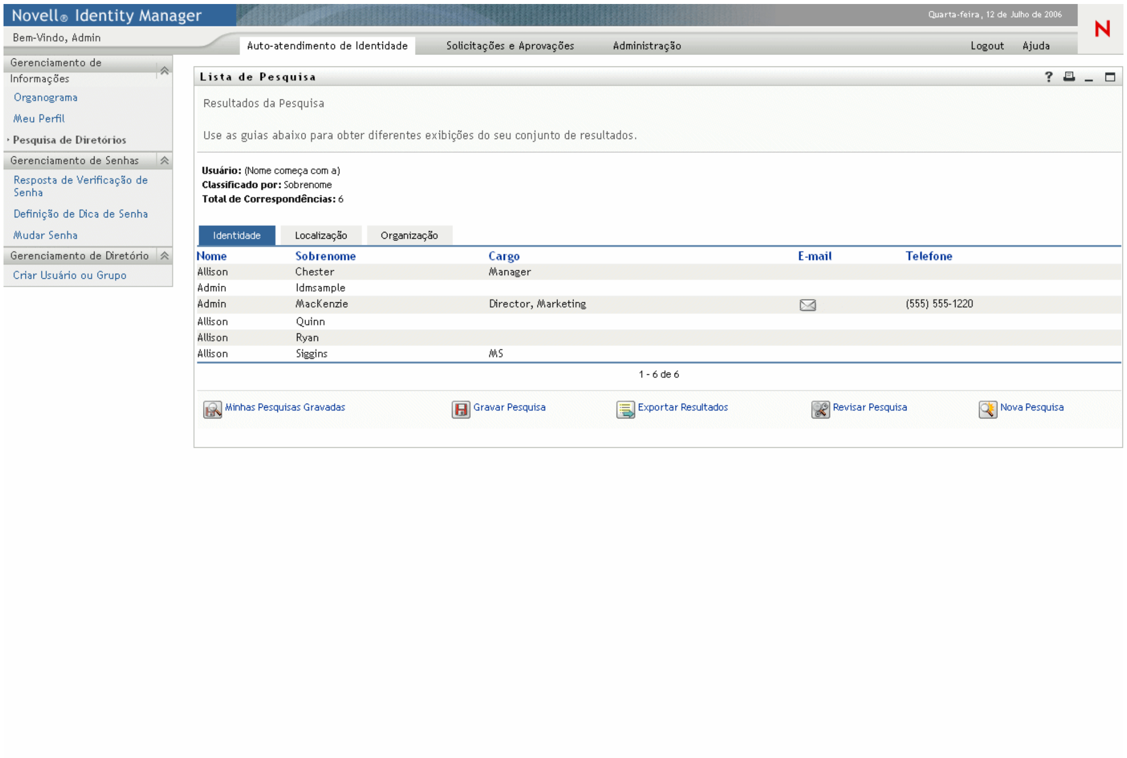
O portlet *Lista de Pesquisa* permite que os usuários pesquisem e exibam o conteúdo do cofre de identidade. É a base da ação *Pesquisa de Diretórios* da guia Auto-atendimento de Identidade do aplicativo de usuário do Identity Manager. A ação da Pesquisa de Diretórios é configurada para que os usuários possam procurar usuários, grupos e grupos de tarefas. Entretanto, você pode modificá-la a fim de mudar o escopo dos atributos e objetos pesquisáveis.

O exemplo a seguir mostra como a ação da Pesquisa de Diretórios permite aos usuários definir os critérios de pesquisa.



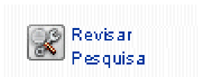
Elemento da interface de usuário	Descrição
Procurar	Os usuários selecionam o tipo de objeto a pesquisar. Para obter mais informações sobre como definir o conteúdo da lista, consulte a Seção 20.2.2, “Definindo preferências da Lista de Pesquisa” na página 298.
Com estes critérios	Para definir os critérios de pesquisa, os usuários selecionam os atributos e os operadores de pesquisa na lista suspensa. Na Pesquisa Avançada, o usuário pode especificar diversas linhas e diversos blocos de agrupamentos de critérios de pesquisa que podem ser inclusivos (E) ou exclusivos (OU). Para obter mais informações sobre como definir os atributos pesquisáveis, consulte a Seção 20.2.2, “Definindo preferências da Lista de Pesquisa” na página 298.
Pesquisar	Executa os critérios de pesquisa especificados. Para obter mais informações sobre como definir a pesquisa padrão, consulte a Seção 20.2.2, “Definindo preferências da Lista de Pesquisa” na página 298.
Minhas Pesquisas Gravadas 	Permite ao usuário executar, editar ou excluir uma pesquisa selecionada e já gravada.
Pesquisa Avançada 	Como o botão Pesquisar, ela permite que o usuário adicione linhas ou blocos de critérios de pesquisa, mas em uma pesquisa avançada, eles podem especificar diversas linhas e diversos blocos de agrupamentos de critérios de pesquisa que podem ser inclusivos (E) ou exclusivos (OU). Para obter mais informações sobre como definir os atributos pesquisáveis, consulte a Seção 20.2.2, “Definindo preferências da Lista de Pesquisa” na página 298.

Este exemplo mostra como o portlet é exibido (com exemplos de dados) depois que o critério de pesquisa *Nome começa com A* é especificado:



Você pode configurar o portlet Lista de Pesquisa para usar um destes recursos:

Elemento da interface de usuário	Descrição
Guias Identidade, Localização, Organização	Os usuários clicam em uma dessas guias para ver a lista de resultados exibida de diversas maneiras. Para obter mais informações sobre formatos, consulte a Seção 20.1.1, “Sobre os formatos de exibição da lista de pesquisa” na página 294.
Minhas Pesquisas Gravadas 	Permite ao usuário selecionar uma pesquisa já gravada.
Gravar Pesquisa 	Permite aos usuários gravar critérios de pesquisa e reexecutar pesquisas gravadas, caso seja necessário. As pesquisas são gravadas no atributo srvprvQueryList do usuário conectado.
Exportar Resultados 	Permite aos usuários exportar os resultados de pesquisa para outro formato.

Elemento da interface de usuário	Descrição
Revisar Pesquisa 	Permite aos usuários mudar os critérios de pesquisa.
Nova Pesquisa 	Permite ao usuário definir uma nova pesquisa.

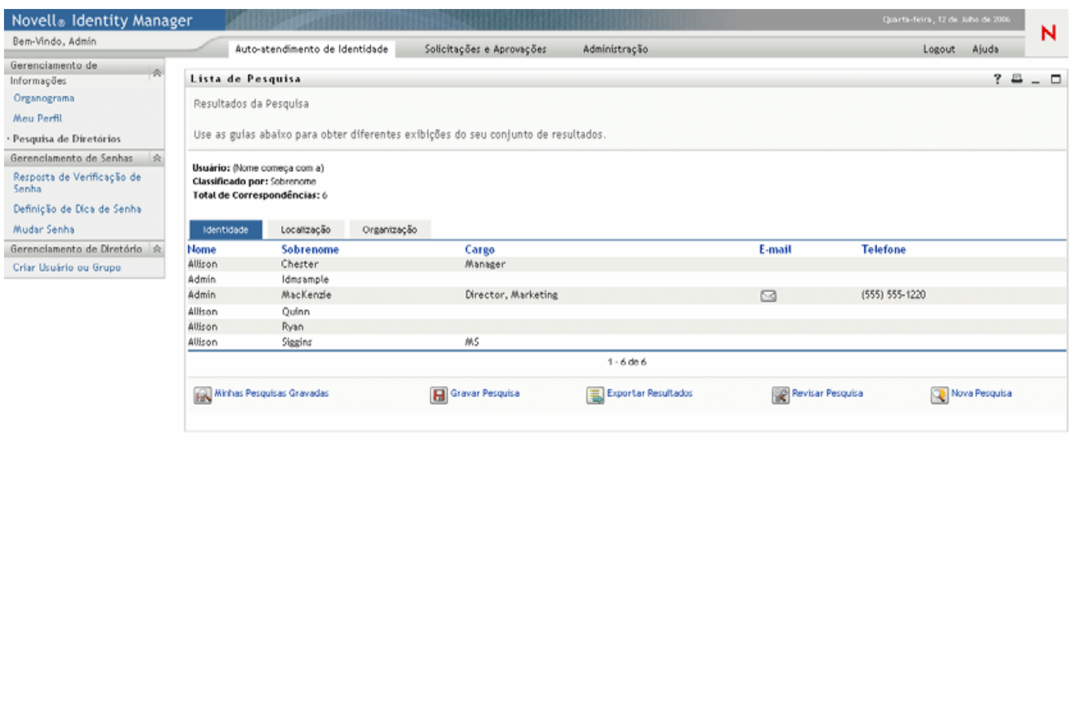
Por padrão, a Lista de Pesquisa também permite aos usuários finais:

- Imprimir os resultados de pesquisa
- Iniciar e-mails na lista de resultados
- Iniciar o portlet Detalhes na lista de resultados

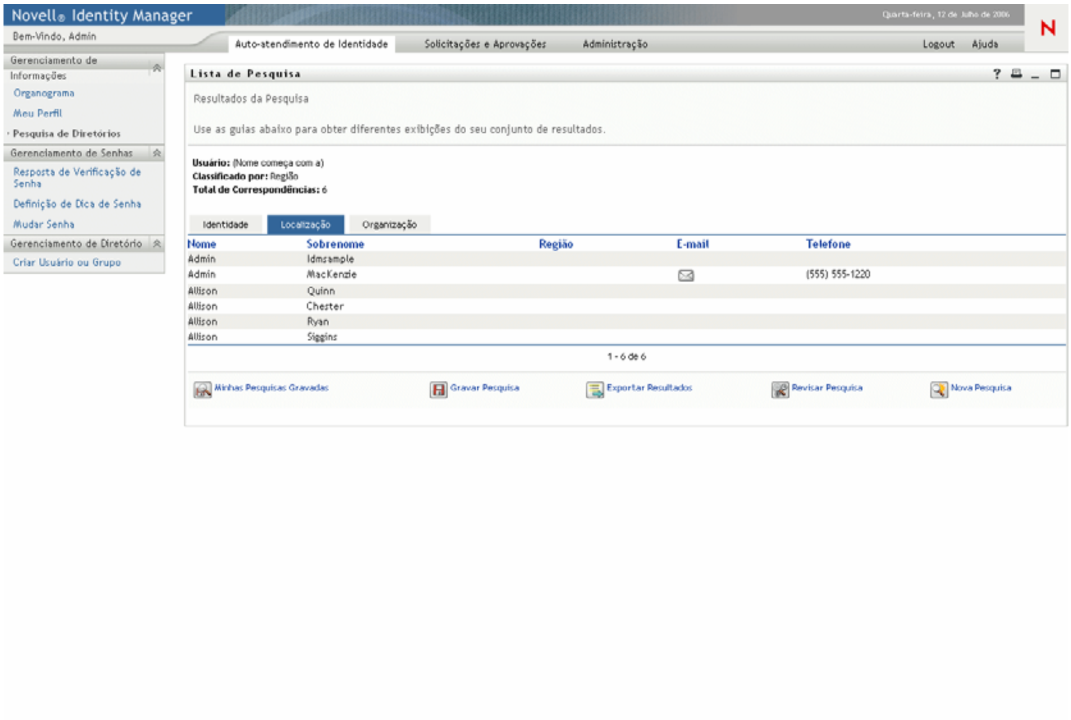
20.1.1 Sobre os formatos de exibição da lista de pesquisa

É possível definir como os dados retornados pela pesquisa no cofre de identidade serão exibidos aos usuários finais. Os dados podem ser organizados em um ou mais destes tipos de página:

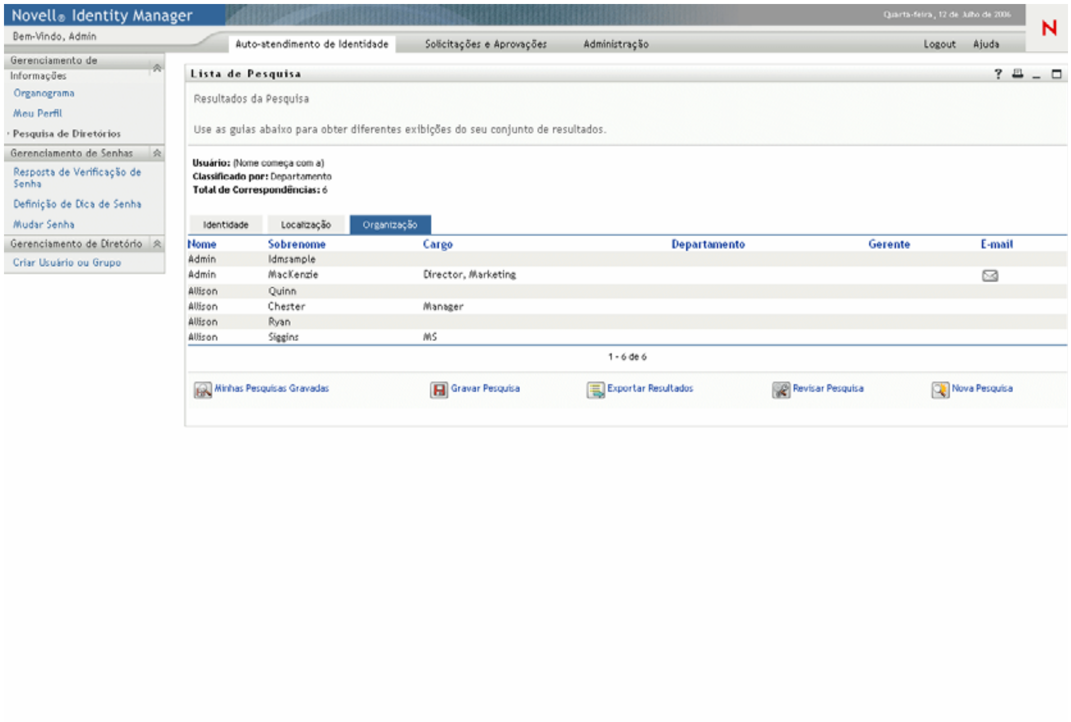
- *Páginas de Identidade* — Normalmente inclui informações de contato, como mostra abaixo:



- *Páginas de Localização* — Normalmente inclui informações de localização, como mostra abaixo:



- *Páginas de Organização* — Normalmente inclui informações de hierarquia da organização, como mostra abaixo:



Você pode definir outros formatos da lista de resultados com as preferências complexas do portlet. Por exemplo, se o esquema do cofre de identidade inclui informações sobre habilidades ou certificações do funcionário, você pode configurar uma lista de resultados para exibir essas informações.

Dependendo de como você configurar o portlet, os usuários finais poderão:

- Escolher os tipos de objetos do cofre de identidade para pesquisa (como usuários e grupos)
- Especificar os *critérios* a serem usados para pesquisa (como, Nome começa com, Sobrenome incluir, e assim por diante)
- Escolher o *formato de exibição* para os resultados da pesquisa
- Mudar a *ordem de classificação*

20.2 Configurando o portlet Lista de Pesquisa

Para configurar o portlet Lista de Pesquisa, você seguirá um conjunto de etapas como este:

Etapa	Tarefa	Descrição
1	Definir: ◆ As entidades e os atributos que os usuários poderão pesquisar. ◆ Como a lista de resultados será exibida	Você pode usar a ação da Pesquisa de Diretórios que é instalada com o aplicativo de usuário do Identity Manager como está. É possível modificá-la ou criar uma própria. Para obter mais informações, consulte a Seção 20.2.2, “Definindo preferências da Lista de Pesquisa” na página 298.
2	Verificar se o conjunto de entidades e atributos para a pesquisa são definidos na camada de abstração do diretório.	Para obter mais informações, consulte o Capítulo 4, “Configurando a Camada de Abstração do Diretório” na página 75.
3	Determinar como os usuários devem acessar o portlet:	Os usuários poderão iniciar o portlet em uma página nova ou uma página existente? Para obter mais informações sobre páginas, consulte o Capítulo 7, “Administração de Página” na página 137.
4	Definir preferências para o portlet	As preferências do portlet Lista de Pesquisa permitem definir: ◆ Os atributos exibidos para cada formato da lista de resultados. ◆ Que formato de exibição da lista de resultados será produzido por uma pesquisa ◆ A ordem de classificação padrão dos formatos da lista de resultados Para obter mais informações, consulte a Seção 20.2.2, “Definindo preferências da Lista de Pesquisa” na página 298.
5	Testar as configurações	Verifique se as listas de resultados mostram os atributos desejados.
6	Definir os direitos do eDirectory e estabelecer os índices necessários para melhorar o desempenho	Direitos do eDirectory: Para executar uma pesquisa ◆ O usuário que executa a pesquisa precisa ter direitos de **Pesquisar** para os usuários ou objetos que estão sendo pesquisados. Para gravar uma pesquisa (para usuários não administrativos): ◆ **Trustee** da unidade organizacional e a organização onde a pesquisa será executada. ◆ **Usuário** requer direitos de gravação, de usuário e de supervisor. **Aprimoramento do desempenho —** O desempenho da pesquisa pode ser melhorado com a inclusão do índice de valores do eDirectory no atributo em que a pesquisa se baseia.

Para obter mais informações sobre como definir diferentes formatos de exibição da lista de resultados, consulte a Seção 20.2.2, “Definindo preferências da Lista de Pesquisa” na página 298.

20.2.1 Configuração da camada de abstração do diretório

As entidades e os atributos que podem ser selecionados na lista suspensa de critérios de pesquisa e os dados retornados pelas pesquisas do cofre de identidade devem ser definidos na camada de abstração do diretório. A tabela a seguir mostra as propriedades que devem ser definidas para as entidades e os atributos usados pela lista de pesquisa.

Tipo de definição	Configuração	Valor da camada de abstração do diretório
entidade	exibir	Marcado (verdadeiro)
atributo	habilitar	Marcado (verdadeiro)
	pesquisar	Marcado (verdadeiro) Se for falso, você não poderá definir uma pesquisa neste atributo ou incluí-lo em um formato da lista de resultados
	ocultar	Desmarcado (falso) Qualquer atributo em que a pesquisa seja selecionada (verdadeiro) também deve ter ocultar definido como desmarcado (falso), pois o portlet Lista de Pesquisa não examina o valor da propriedade ocultar durante a pesquisa (porque ele prejudica o desempenho). Suponha que o Usuário 1 defina o atributo HomePhone seja ocultar=verdadeiro (no eDirectory). HomePhone pode ser pesquisado, de forma que a Lista de Pesquisa recupera o registro, mas não examina os valores dos outros atributos (devido ao impacto causado no desempenho). Se outro usuário pesquisar uma correspondência exata do atributo HomePhone, o registro oculto será exibido na lista de resultados.

Outras configurações da camada de abstração do diretório O tipo de dados, o tipo de formato, os filtros e o escopo da pesquisa da camada de abstração do diretório também causarão impacto no portlet Lista de Pesquisa. O tipo de dados e de formato afetam a aparência, o filtro e escopo da pesquisa afetarão como os dados serão retornados.

Para obter mais informações, consulte a Seção 4.3, “Trabalhando com entidades e atributos” na página 87.

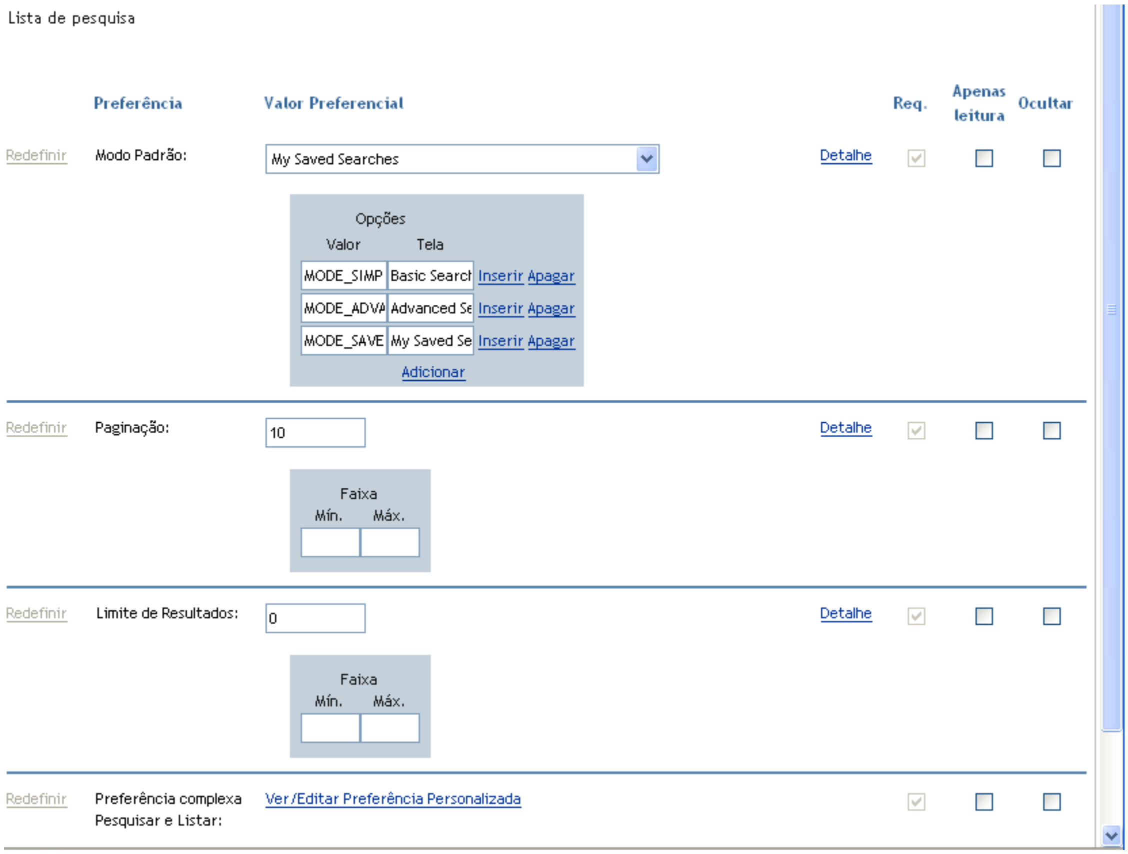
20.2.2 Definindo preferências da Lista de Pesquisa

Você define dois tipos de preferências:

- “Preferências de pesquisa” na página 299
- “Preferências de formato da lista de resultados” na página 301

Preferências de pesquisa

As preferências de pesquisa estão contidas em uma única página de preferências:



As preferências de pesquisa são definidas abaixo:

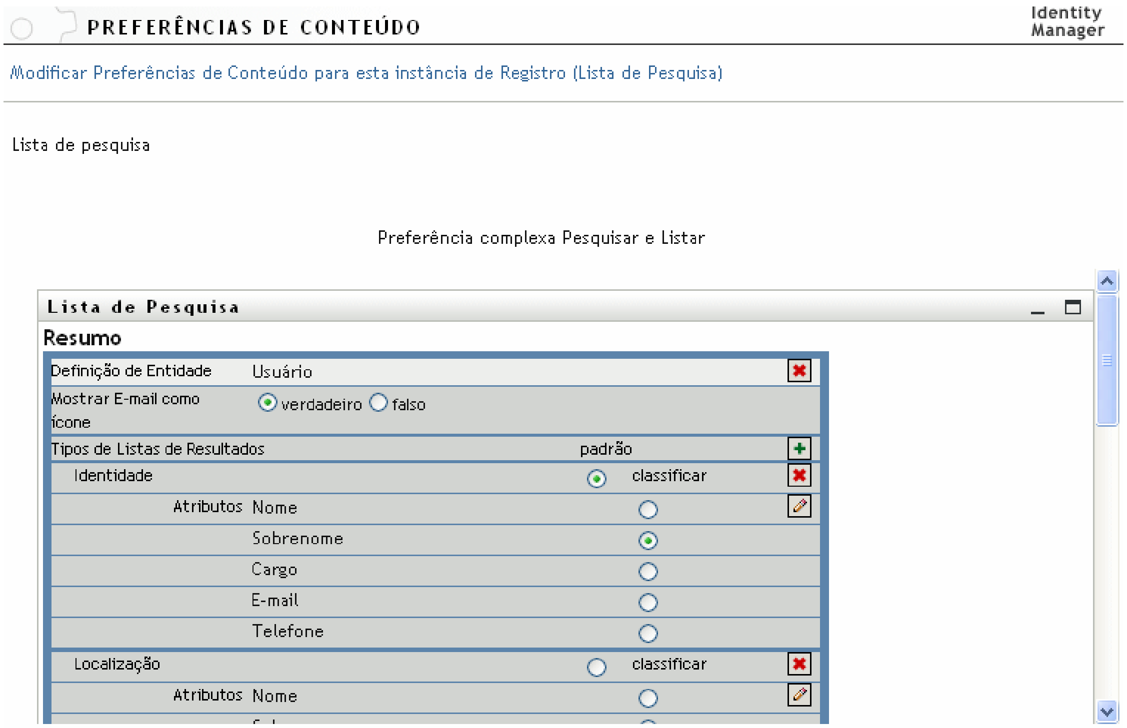
Preferência	O que fazer

Modo Padrão	Especifique como deseja que o portlet seja exibido quando um usuário o acessar pela primeira vez. Os valores são:
	
	Pesquisa Básica — Permite que os usuários informem um único critério de pesquisa. Por exemplo:
	
	`Nome começa com A`
	
	Pesquisa Avançada — Permite que os usuários definam diversos critérios de pesquisa em um ou mais blocos. Os usuários podem usar os operadores lógicos e/ou nos critérios de pesquisa ou entre os blocos de pesquisa. Por exemplo, os usuários podem criar uma pesquisa como esta:
	
	`(Nome começa com A ou Nome começa com B) e (Região= Nordeste ou Região = Sudeste)`
	
	OU
	
	`(Nome começa com A e Sobrenome começa com B) ou (Nome começa com B e Sobrenome começa com A)`
	
	Minhas Pesquisas Gravadas — Exibe uma lista de pesquisas gravadas pelo usuário conectado. As pesquisas são gravadas no atributo srvprvQueryList do usuário conectado.
	
	Observação: Os usuários podem acessar todos esses modos em tempo de execução por meio da execução ou edição de uma pesquisa ou ao clicar em um botão na parte inferior do portlet.

Paginação	O número máximo de linhas exibidas de uma vez.
Limite de Resultados	O número máximo de correspondências retornadas pela pesquisa. Se o valor for definido como 0, o máximo passa a ser a configuração da camada de abstração do diretório.
Preferência complexa da Lista de Pesquisa	Clique para refinar: ◆ As entidades a serem pesquisadas ◆ O tipo do conjunto de resultados ◆ Os atributos a serem incluídos nas páginas e a ordem em que eles aparecem Por padrão, todos os objetos listados na camada de abstração do diretório com o atributo exibir=verdadeiro são incluídos na pesquisa. A lista de atributos da entidade deriva-se dos atributos relacionados na camada de abstração do diretório e que estão definidos como habilitar=verdadeiro.

Preferências de formato da lista de resultados

A página de preferências complexas permite definir as entidades a serem incluídas na pesquisa e como formatar a lista de resultados. Esta é a aparência da página de preferências padrão:



As preferências complexas incluem:

Preferência	O que fazer
Definição de Entidade	Todo objeto válido para pesquisa (exibir=verdadeiro) tem um bloco de Definição de Entidade correspondente nesta página de preferências. Use as preferências para: ◆ Definir os objetos incluídos na pesquisa. ◆ Modificar as definições de formato da lista de resultados (como adicionar e remover os atributos exibidos e sua ordem de classificação padrão). ◆ Remover os objetos que não serão incluídos na pesquisa clicando no botão apagar que aparece na linha Definição de Entidade. O bloco de definição de entidade inteiro é apagado. Você pode adicionar o objeto novamente à pesquisa. Para isso, clique em **Adicionar Definição de Entidade** (localizada na parte inferior da página) e preencha os painéis de seleção do assistente. **Dica:** Se um objeto não aparecer na lista, mas estiver relacionado na camada de abstração do diretório, marque o modificador **exibir**(no objeto Entidade). Se estiver definido como falso, a entidade não poderá ser usada pelos portlets de identidade.
Mostrar e-mail como ícone	Quando verdadeiro e se houver um atributo E-mail especificado na lista de resultados, será exibido como um ícone. Quando falso, o atributo E-mail exibirá o endereço de e-mail completo. O atributo de e-mail (seja texto ou ícone) é um link mailto: em que se pode clicar.
Tipos de Lista de Resultados (padrão)	Especifica o formato padrão da lista de resultados da entidade atual. O padrão só é usado quando nenhum outro formato é selecionado pelo usuário.
Blocos de formato de exibição da Lista de Pesquisa	Especifica o formato de exibição (como páginas Identidade, Localização ou Organizacional) e inclui o conjunto de atributos a serem incluídos para o tipo. **Para remover um tipo de lista de resultados:** ◆ Clique no botão apagar ao lado do Tipo de Lista de Resultados. O tipo de página e todos os atributos associados são apagados da pesquisa. **Para adicionar uma página de conjunto de resultados:** ◆ Clique no botão expandir e selecione o formato do conjunto de resultados na lista de opções.

Preferência	O que fazer
Atributos	Especifica o conjunto de atributos que aparecerão para o formato de exibição específico. **Para adicionar ou remover um atributo:** ◆ Clique no botão modificar atributos. ◆ Para adicionar um atributo, selecione-o (na lista de atributos disponíveis). ◆ Clique na seta para movê-lo para a lista Selecionado. Faça o inverso para remover um atributo na Lista de Resultados. ◆ Para reordenar a lista de atributos, clique nas setas para cima e para baixo à direita da lista selecionada. ◆ Clique em **Submeter**. **Atributos e tipos de dados** — O tipo de dados do atributo afeta a maneira como eles são exibidos. Por exemplo, se um atributo é definido como um subtipo de uma lista local ou uma lista global, os valores possíveis serão exibidos em uma caixa de listagem suspensa nas telas Critérios de Pesquisa Básica ou Avançada. Se o tipo for DN, um botão de localização e histórico será exibido para que os usuários possam selecionar um valor nas telas Critérios de Pesquisa Básica ou Avançada, e o DN será resolvido em uma tela simples na lista de resultados. O tipo e o subtipo dos dados também restringem o operador de comparação exibido para o usuário a fim de garantir que somente comparações válidas sejam elaboradas. Para obter mais informações, consulte o Capítulo 4, “Configurando a Camada de Abstração do Diretório” na página 75.
Classificação de blocos de formato de exibição da Lista de Pesquisa	A ordem de classificação da lista de resultados baseia-se neste atributo. A ordem de classificação padrão só será ativada se o Tipo de Conjunto de Resultados não for o formato de exibição da atual sessão do usuário. **Atributos de vários valores e atributos de valor único** — O número de registros exibidos em uma lista de resultados varia caso o atributo de classificação tenha valor único ou múltiplo. Classificar com atributos de vários valores em geral parece resultar em mais registros, embora o número total de correspondência seja o mesmo. Isso ocorre porque cada valor de um atributo com vários valores aparece em uma linha individual.

Preenchendo o painel de preferências

Para verificar se você enviou as entradas válidas, clique em *Submeter*. Se uma entrada não é válida, você verá uma mensagem de erro na parte superior da página de preferências. Depois de solucionar todos os erros, clique em *Retorne à Tela de Lista* e clique em *Gravar Preferências*.

Criando e gerenciando solicitações de aprovisionamento

V

Estes capítulos ensinam a usar os recursos do Módulo de Aprovisionamento do Identity Manager.

Introdução ao aprovisionamento com base em workflow

21

Este capítulo fornece uma visão geral do aprovisionamento com base em workflow. Os tópicos incluem:

21.1 Sobre o aprovisionamento com base em workflow

Um recurso importante do Identity Manager é o *aprovisionamento com base em workflow*, que é o processo de gerenciar o acesso do usuário a recursos seguros de uma organização. Esses recursos podem incluir entidades digitais, como contas de usuário, computadores e bancos de dados. Nesta versão, os recursos aprovisionados são mapeados para direitos do Identity Manager.

O Identity Manager pode atender a uma grande variedade de *solicitações de aprovisionamento*. As solicitações de aprovisionamento são ações do usuário ou do sistema destinadas a conceder ou revogar o acesso a recursos organizacionais. Elas podem ser iniciadas diretamente pelo usuário final através do aplicativo de usuário do Identity Manager, ou indiretamente em resposta a eventos que ocorrem no cofre de identidade (eDirectory).

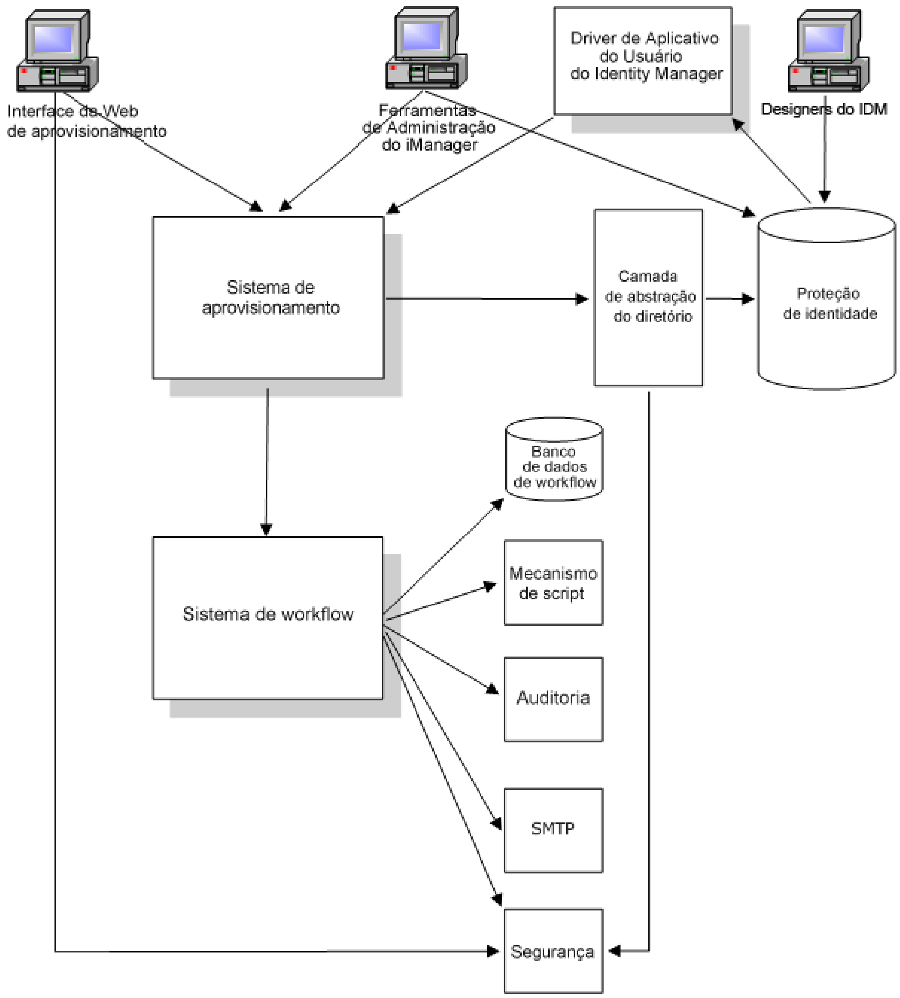
Quando uma solicitação de aprovisionamento requer permissão de uma ou mais pessoas em uma organização, a solicitação inicia um workflow. O workflow coordena as *aprovações* necessárias para atender à solicitação. Algumas solicitações de aprovisionamento requerem aprovação de uma única pessoa, enquanto outras requerem aprovação de várias. Em algumas situações, uma solicitação pode ser atendida sem aprovações.

Certos workflows precisam que o processamento prossiga de forma *seqüencial*, com cada etapa de aprovação realizada em seqüência. Outros workflows dão suporte ao processamento *paralelo*. Ao definir uma solicitação de aprovisionamento, você especifica se deseja que o workflow aceite o processamento seqüencial ou paralelo.

O Identity Manager oferece um conjunto de ferramentas baseadas na Web que o administrador pode usar para gerar recursos de aprovisionamento no aplicativo de usuário. Essas ferramentas permitem que você configure solicitações de aprovisionamento e também gerencie workflows que estejam em andamento. Para configurar uma solicitação de aprovisionamento, o administrador cria uma *definição de solicitação de aprovisionamento*, que vincula o recurso a um workflow.

21.1.1 Arquitetura de alto nível

O seguinte diagrama mostra a arquitetura de alto nível do sistema de aprovisionamento com base em workflow incluído no Identity Manager:



As seções a seguir descrevem cada componente da arquitetura.

Interface da Web para o aprovisionamento

O aplicativo de usuário do Identity Manager fornece uma interface da Web pela qual os usuários finais submetem solicitações de aprovisionamento e gerenciam essas solicitações depois que elas são submetidas. O aplicativo de usuário também oferece o Administrador de Aplicativo de Usuário ou um Gerente Organizacional capaz de designar delegados e proxies aos workflows de aprovisionamento.

Dica: As ações de aprovisionamento e workflow estão disponíveis na guia *Solicitações e Aprovações* do aplicativo de usuário do Identity Manager.

Para obter mais informações sobre delegados e proxies, consulte a Seção 21.3, “Segurança de aprovisionamento” na página 317. Para obter detalhes completos sobre como trabalhar com o aplicativo de usuário, consulte o *Aplicativo de Usuário do Identity Manager: Guia do Usuário*.

Ferramentas de administração do iManager

O iManager contém plug-ins que você pode usar para configurar e gerenciar solicitações de aprovisionamento e os workflows associados.

Para configurar uma solicitação de aprovisionamento, vincule-a a um recurso aprovisionado, especifique as características de tempo de execução do workflow associado e habilite-a para uso. Depois que uma solicitação de aprovisionamento é iniciada, você pode usar o iManager para ver o status do processo de workflow, redesignar atividades no workflow ou encerrar um workflow que esteja obstruído.

Driver de Aplicativo do Usuário do Identity Manager

Além do suporte a solicitações do usuário final por recursos de aprovisionamento, o Identity Manager permite que você inicie solicitações de aprovisionamento em resposta a eventos que ocorrem no eDirectory. O *Driver de Aplicativo do Usuário* do Identity Manager recebe eventos e responde ao iniciar as solicitações de aprovisionamento correspondentes. As solicitações, por sua vez, iniciam workflows para administrar o processo de aprovação. Por exemplo, caso o tenha configurado para tal, o Identity Manager dará suporte a situações em que a inclusão de um novo usuário no eDirectory aciona automaticamente um workflow e uma solicitação de aprovisionamento previamente designados.

Sistema de Aprovisionamento

O Sistema de Aprovisionamento executa todo o processamento necessário para iniciar solicitações de aprovisionamento e atendê-las. Se uma solicitação exigir uma ou mais aprovações, o Sistema de Aprovisionamento chamará o Sistema de Workflow para que inicie o processo de workflow. Depois das aprovações necessárias serem obtidas, o Sistema de Aprovisionamento fornece os recursos como solicitado.

O Sistema de Aprovisionamento mantém informações sobre solicitações de aprovisionamento disponíveis e pendentes no cofre de identidade (eDirectory).

Para iniciar uma solicitação ou executar o processamento necessário para cumprir uma solicitação, o sistema acessa o cofre de identidade através da Camada de Abstração do Diretório.

Para obter detalhes sobre a Camada de Abstração do Diretório, consulte o Capítulo 4, "Configurando a Camada de Abstração do Diretório" na página 75.

Sistema de Workflow

Quando uma solicitação de aprovisionamento requer uma ou mais aprovações, o Sistema de Workflow coordena o processo de aprovação. Durante o processamento, ele interage com estes componentes:

- Banco de dados de workflow
- Mecanismo de script
- Audit
- SMTP
- Sistema de segurança

Banco de dados de workflow

Para monitorar o estado dos workflows em processamento, o Sistema de Workflow armazena informações em um banco de dados. Esse banco de dados mantém informações sobre instâncias do processo de workflows, listas de trabalho (filas) e destinatários do workflow. Ele também armazena comentários adicionados durante a execução de um processo de workflow.

Mecanismo de script

O Sistema de Workflow chama o Mecanismo de Script toda vez que um workflow inclui uma expressão dinâmica que precisa ser avaliada. Expressões dinâmicas podem incluir variáveis, funções e operadores, bem como referências a entidades da Camada de Abstração do Diretório.

Novell Audit

Para registrar informações sobre o estado de um processo de workflow, o Sistema de Workflow interage com o Novell Audit. Durante seu processamento, o workflow pode registrar informações sobre vários eventos que tenham ocorrido. Os usuários podem, então, usar as ferramentas de relatório do Novell Audit para verificar os dados do registro.

Para obter detalhes sobre como configurar registros, consulte o Capítulo 5, “Configurando o registro” na página 119. Para obter detalhes sobre como controlar os níveis de mensagens de registro que o aplicativo de usuário do Identity Manager deve gerar, consulte o Capítulo 12, “Configuração de Registro” na página 211.

SMTP

Em geral, o processo de workflow envia notificações por e-mail em vários pontos durante sua execução. Por exemplo, um e-mail pode ser enviado quando uma atividade de workflow é atribuída a um novo destinatário.

O administrador pode editar um gabarito de e-mail no iManager e depois usar esse gabarito em um processo de workflow. No tempo de execução, o Sistema de Workflow o recupera no eDirectory e substitui as tags por texto dinâmico adequado à notificação.

As notificações por e-mail são tratadas pelo protocolo SMTP (Simple Mail Transfer Protocol).

Para informar-se sobre as etapas básicas de configuração da notificação por e-mail, consulte a Seção 23.3, “Configurando o servidor de e-mail” na página 352 e a Seção 23.4, “Trabalhando com o gabarito de e-mail instalado” na página 353. Para obter detalhes sobre como configurar a notificação por e-mail para um workflow, consulte “Configurando as atividades de workflow” na página 334.

Segurança

O sistema de segurança trata de todos os aspectos de segurança de um aplicativo de aprovisionamento que utiliza workflows.

Para obter mais informações sobre segurança de workflow, consulte a Seção 21.3, “Segurança de aprovisionamento” na página 317.

21.1.2 Exemplo de aprovisionamento e workflow

Suponha que um usuário precise de uma conta em um sistema de TI. Para configurar a conta, o usuário inicia uma solicitação pelo aplicativo de usuário do Identity Manager. Essa solicitação gera

um workflow, que coordena um processo de aprovação. Depois das aprovações necessárias serem concedidas, a solicitação é atendida. Estas são as três etapas básicas do processo.

Etapa 1: Iniciando a solicitação

No aplicativo de usuário do Identity Manager, o usuário procura uma lista de recursos por *categoria* e seleciona uma para fornecer. No cofre de identidade, o *recurso aprovisionado* selecionado é associado a uma *definição de solicitação de aprovisionamento*. A definição de solicitação de aprovisionamento é o objeto mais proeminente de um sistema de aprovisionamento. Ela vincula um recurso aprovisionado a um *workflow* e atua como o meio pelo qual o processo de workflow é exposto ao usuário final. A definição de solicitação de aprovisionamento fornece todas as informações necessárias à exibição do *formulário de solicitação inicial* ao usuário, e ao início do fluxo que se segue à solicitação inicial.

No exemplo, o usuário seleciona o recurso Nova Conta. Quando o usuário inicia a solicitação, o aplicativo Web recupera o formulário de solicitação inicial e a descrição dos *dados da solicitação inicial* associados no Sistema de Aprovisionamento, que obtém esses objetos na definição de solicitação de aprovisionamento.

Quando uma solicitação de aprovisionamento é iniciada, o Sistema de Aprovisionamento controla o iniciador e o destinatário. O *iniciador* é a pessoa que fez a solicitação. O *destinatário* é a pessoa para a qual a solicitação foi feita. Em algumas situações, o iniciador e o destinatário podem ser a mesma pessoa.

Cada solicitação de aprovisionamento tem uma *operação* associada. A operação especifica se o usuário deseja *conceder* ou *revogar* o recurso.

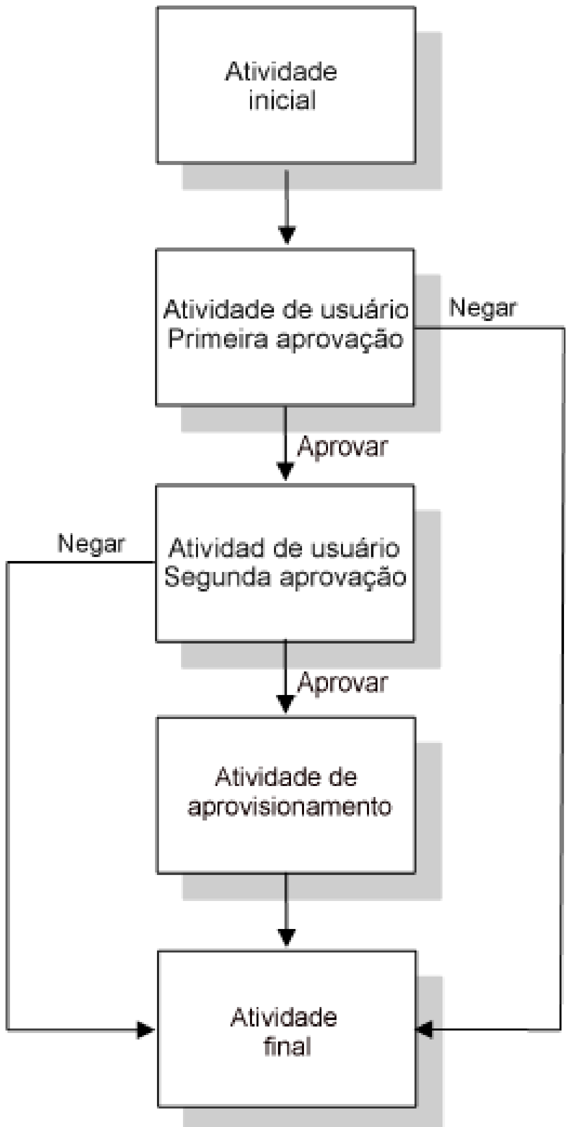
Etapa 2: Aprovando a solicitação

Depois que o usuário iniciar uma solicitação, o Sistema de Aprovisionamento inicia o processo de workflow. O *processo de workflow* coordena as aprovações. No exemplo, são necessários dois níveis de aprovações, um do gerente do usuário e outro do supervisor do gerente. Se a aprovação for recusada por qualquer usuário em um workflow, o fluxo é encerrado e a solicitação é negada.

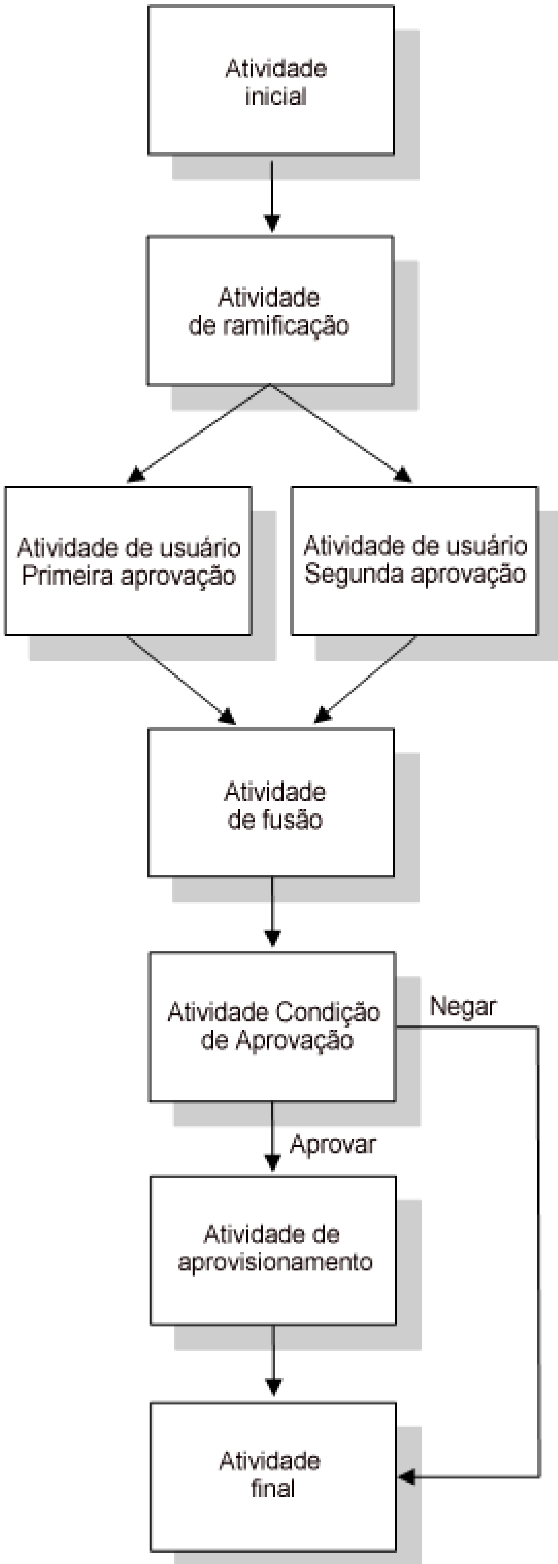
Observação: O Identity Manager é fornecido com um conjunto de gabaritos de solicitações de aprovisionamento que suporta cinco níveis de aprovação de workflow. Em uma versão seguida do Identity Manager, o ambiente de design baseada no Eclipse fornecerá as ferramentas que lhe permitem criar seus próprios processos de workflow personalizados. Para obter mais informações sobre os gabaritos fornecidas com esta versão, consulte a Seção 22.2, “Trabalhando com os gabaritos instalados” na página 322.

Os workflows podem processar aprovações de forma seqüencial ou paralela. Em um *workflow seqüencial*, cada tarefa de aprovação deve ser processada antes do início da próxima tarefa de aprovação. Em um *workflow paralelo*, os usuários podem trabalhar nas tarefas de aprovação simultaneamente.

Fluxo seqüencial Este é o padrão de design básico de um workflow seqüencial com duas aprovações:



Fluxo paralelo Este é o padrão de design básico de um workflow paralelo com duas aprovações:



Observação: As etiquetas de exibição (Primeira aprovação, Segunda aprovação e assim por diante) podem ser facilmente mudadas para que atendam aos requisitos do aplicativo. Para os fluxos

paralelos, convém especificar etiquetas que não impliquem processamento seqüencial. Por exemplo, você pode atribuir etiquetas como Uma das Três Aprovações Paralelas, Duas de Três Aprovações Paralelas e assim por diante.

A definição de workflow é formada pelos seguintes componentes

Componentes do processo	Descrição
Atividades	Uma atividade é um objeto que representa uma tarefa. Uma atividade pode apresentar informações ao usuário e responder a interações do usuário, ou executar funções em segundo plano que não são visíveis ao usuário. Nos exemplos de workflow exibidos abaixo, as atividades são representadas por caixas. No aplicativo de usuário do Identity Manager, as atividades do usuário que lidam com o processo de aprovação são chamadas de **tarefas**. Um usuário final pode ver a lista de tarefas em sua fila ao clicar em **Minhas Tarefas** no grupo de ações de **Meu Trabalho**. Para ver quais atividades de workflow foram processadas por determinada tarefa, o usuário pode selecionar a tarefa e clicar no botão **Ver Histórico de Comentários** do formulário Detalhe da Tarefa. Para ver quais atividades de workflow foram processadas para determinada solicitação de aprovisionamento, o usuário pode clicar em **Minhas Solicitações**, selecionar a solicitação e clicar no botão **Ver Comentário e Histórico de Fluxo** do formulário Detalhe da Solicitação. Para obter mais informações sobre as ações **Minhas Tarefas** e **Minhas Solicitações**, consulte o Aplicativo de Usuário do *Identity Manager: Guia do Usuário*.
Links	Os links vinculam as atividades em um workflow. Um link representa um caminho a ser seguido entre duas atividades. Uma atividade pode ter diversos links de entrada e vários links de saída. Quando uma atividade tem mais de um link de saída, o link selecionado dependerá do **resultado** da atividade. O resultado é proveniente do processamento realizado pela atividade. Por exemplo, uma atividade do usuário pode ter um resultado aprovado ou negado, dependendo da **ação** executada pelo usuário. Nos exemplos de workflow exibidos abaixo, os links são representados por setas.

Atividade inicial O processo de workflow começa com a execução da *atividade inicial*. Essa atividade abre um documento de trabalho que utiliza os dados da solicitação inicial. Ela também vincula diversos valores do sistema, como o iniciador e o destinatário, de forma que eles possam ser usados em expressões de script.

Atividades do usuário Depois que a atividade inicial é executada, o Sistema de Workflow encaminha o processamento para a primeira *atividade do usuário* no fluxo. A atividade do usuário dá suporte a interações do usuário. Para lidar com essas interações, a atividade exibe um formulário que permite ao usuário trabalhar com a solicitação. Nos exemplos de workflow exibidos acima, a `Primeira aprovação` e a `Segunda aprovação` são exemplos de atividades do usuário. As etiquetas de exibição das atividades do usuário podem ser localizadas de forma a atender requisitos internacionais.

Uma atividade do usuário pode suportar uma ou mais destas *ações*:

- Requerer
- Aprovar
- Negar
- Recusar
- Reatribuir (disponível somente aos Gerentes Organizacionais e aos Administradores de Aplicativo de Usuário)

Observação: Os campos e os botões do formulário variarão de acordo com o recurso solicitado e com a configuração do workflow. A ação *Recusar*, por exemplo, não tem suporte em muitos gabaritos fornecidos com o produto.

Uma atividade do usuário tem cinco *resultados* possíveis:

- Aprovado
- Negado
- Recusado
- Erro
- Tempo de Espera

Observação: Os resultados Erro e Tempo de Espera podem ocorrer sem qualquer ação executada pelo usuário.

Se o usuário aprovar a solicitação, o workflow encaminhará o controle para a próxima atividade do fluxo. Se mais nenhuma aprovação for necessária, o recurso será aprovisionado. Se o usuário negar a solicitação, o item de trabalho será encaminhado para a próxima atividade do workflow e a solicitação será negada. O usuário também tem a alternativa de reatribuir a tarefa (se ele é um Gerente Organizacional ou um Administrador de Aplicativo de Usuário), que coloca o item de trabalho na fila de outro usuário.

Observação: Os gabaritos de solicitação de aprovisionamento fornecidos com o produto são configurados para encerrar um processo de workflow quando uma solicitação é negada. Quando uma solicitação é negada, o item de trabalho é encaminhado à atividade Concluir, que encerra o fluxo.

O usuário para quem a atividade foi atribuída é o *destinatário*. O destinatário de uma atividade pode ser notificado da tarefa atribuída por meio de e-mail. Para realizar o trabalho associado à atividade, o destinatário pode clicar no URL do e-mail, encontrar a tarefa na lista de trabalho (fila) e requerer a tarefa.

O destinatário deve responder a uma atividade do usuário em um prazo determinado, ou a atividade entra em tempo de espera. Normalmente, o *intervalo de tempo de espera* é expresso em horas ou dias para que o usuário tenha tempo suficiente para responder.

Quando ocorre o tempo de espera de uma atividade, o processo de workflow pode tentar concluir a atividade novamente, dependendo do *total de tentativas* especificado para a atividade. Em algumas situações, o processo de workflow pode ser configurado para escalar uma atividade que tenha entrado em tempo de espera para outro usuário. Nesse caso, a atividade é reatribuída a um novo

destinatário (o gerente do usuário, por exemplo) para que esse usuário tenha a oportunidade de concluir o trabalho. Caso a última tentativa entre em tempo de espera, a atividade pode ser marcada como aprovada ou negada, dependendo da configuração do workflow.

Atividades condicionais Durante a execução, um processo de workflow pode realizar um teste e verificar o resultado para decidir o que será feito em seguida. A *atividade condicional* permite isso. As atividades condicionais usam uma expressão de script para definir a condição a ser avaliada. Nos exemplos de workflow exibidos acima, a `Condição de Aprovação` é um exemplo de atividade condicional.

As atividades condicionais podem ter três *resultados* possíveis:

- Verdadeiro
- Falso
- Erro

Atividades de ramificação e mesclagem Em um workflow que utiliza processamento paralelo, a *atividade de ramificação* permite que dois usuários atuem paralelamente em diferentes áreas do item de trabalho. Depois que os usuários concluem seu trabalho, a *atividade de mesclagem* sincroniza as ramificações de entrada no fluxo.

Atividade de aprovisionamento A *atividade de aprovisionamento* atende à solicitação de aprovisionamento. Essa atividade só é executada se todas as aprovações necessárias são obtidas.

Para obter detalhes sobre a etapa de aprovisionamento, consulte a "Etapa 3: Atendendo à solicitação" na página 316.

Atividade de encerramento A *atividade de encerramento* é a atividade final de um workflow. Depois que todas as atividades de um fluxo forem concluídas e o resultado final do fluxo estiver disponível, a atividade de encerramento poderá ser executada. O Sistema de Workflow pode determinar o estado final do processo ao examinar os links na atividade de encerramento. O estado geral do fluxo é *aprovado* quando um link de aprovação chega à atividade de encerramento. Se algum outro resultado (negar, tempo de espera ou erro) conduzir à atividade de encerramento, o estado geral do fluxo será *negado*.

Quando um processo de workflow alcança a atividade de encerramento com um estado de aprovado, o processo de aprovação é concluído e a solicitação de aprovisionamento pode ser atendida.

Etapa 3: Atendendo à solicitação

Depois que uma solicitação de aprovisionamento é aprovada, o Sistema de Workflow pode começar a etapa de *aprovisionamento*. Nesse momento, o controle retorna ao Sistema de Aprovisionamento.

Para atender à solicitação de aprovisionamento, o Sistema de Aprovisionamento pode executar o direito do Identity Manager ou manipular diretamente um objeto do eDirectory e seus atributos. Durante a etapa de aprovisionamento, ele cria os objetos relacionados e registra os resultados da ação de aprovisionamento no destinatário, como descrito na definição de dados de aprovisionamento. Dependendo de o usuário ter solicitado uma operação de conceder ou revogar, isso pode envolver a configuração ou a remoção do valor de um atributo no destinatário, ou a inclusão de um item (ou sua remoção) em um atributo de vários valores no destinatário. Os atributos envolvidos são do eDirectory (possivelmente disponibilizados pela inclusão de uma classe auxiliar no destinatário). Os valores dos próprios atributos podem ser simples ou de um tipo complexo que permita ao Sistema de Aprovisionamento especificar o valor dos subatributos internos.

21.2 Configuração e administração de aprovisionamento

Para configurar uma definição de solicitação de aprovisionamento, use o iManager para vinculá-la a um recurso aprovisionado, especifique as características de tempo de execução do workflow associado e habilite-a para uso. O Identity Manager é fornecido com um conjunto de definições de solicitações de aprovisionamento e workflows pré-distribuídos. Você pode usá-los como *gabaritos* para a criação de seu próprio sistema de aprovisionamento. Os gabaritos instalados são fáceis de usar, mas também flexíveis o suficiente para atender aos requisitos de uma grande variedade de ambientes comerciais. Para configurar o sistema, defina novos objetos com base nos gabaritos instalados e personalize esses objetos para corresponder às necessidades da sua organização.

Depois que uma definição de solicitação de aprovisionamento é configurada, você pode usar o iManager para ver o status dos processos de workflow em execução, redesignar atividades nos workflows ou encerrar um workflow que esteja obstruído.

Para obter mais informações sobre como usar o iManager para a configuração e o gerenciamento do aprovisionamento, consulte o Capítulo 22, "Configurando definições de solicitação de aprovisionamento" na página 321 e o Capítulo 23, "Gerenciando workflows de aprovisionamento" na página 343.

21.3 Segurança de aprovisionamento

Quando um usuário efetua login no aplicativo de usuário do Identity Manager, o sistema de segurança autentica esse usuário e define os controles de acesso para proteger os objetos Aprovisionamento e Workflow de uso não autorizado. Isso garante que o usuário veja somente as definições de solicitação de aprovisionamento a que obteve acesso. Além de executar serviços de autenticação e autorização para o aplicativo de usuário, o sistema de segurança gerencia as designações de proxy e indicado.

- Um *indicado* é um usuário autorizado a executar o trabalho de outro usuário. Uma atribuição de delegação se aplica a uma definição específica de solicitação de aprovisionamento.
- Um *proxy* é um usuário autorizado a executar todo e qualquer trabalho para um ou mais usuários, grupos ou containers. Diferentemente das atribuições de delegação, as atribuições de proxy independem das definições de solicitação de aprovisionamento e, portanto, se aplicam a todos os trabalhos e todas as configurações.

Se o registro for habilitado, as ações executadas por um proxy ou indicado são registradas juntamente com as ações executadas por outros usuários. Quando uma ação é executada por um proxy ou indicado, a mensagem do registro indica claramente que a ação foi executada por um proxy ou indicado para outro usuário. Além disso, toda vez que uma nova atribuição de proxy ou de delegação é definida, esse evento também é registrado.

Se a definição de solicitação de aprovisionamento for configurada para gerar notificações por e-mail, os proxies (bem como os destinatários) serão notificados por e-mail. Os indicados não são incluídos nas notificações por e-mail.

Funções de segurança do workflow O sistema de segurança reconhece as seguintes funções:

<table>
<tr><th>Função</th><th>Descrição</th><th>Direitos</th></tr>
<tr><td>Administrador de Aplicativo de Usuário</td><td>Usuário Super Admin com direitos administrativos totais.</td><td>O Administrador de Aplicativo de Usuário pode executar estas tarefas no iManager:

◆ Configurar solicitações de aprovisionamento
◆ Gerenciar workflows em andamento

O Administrador de Aplicativo de Usuário pode executar estas tarefas no aplicativo de usuário:

◆ Ver e editar todas as tarefas em todas as filas do workflow.
◆ Definir designações de proxy e indicado para qualquer usuário do sistema.
◆ Ver informações ocultas (atributos ocultos) para qualquer usuário no sistema.
◆ Criar Gerenciadores de Grupo de Tarefas e atribuí-los a grupos. O Administrador de Aplicativo de Usuário é o único usuário que pode criar e atribuir Gerentes de Grupo de Tarefas.

Observação: A guia Administração do aplicativo de usuário do Identity Manager contém ferramentas para a atribuição de direitos para administrar o aplicativo de usuário. Para usar essa guia, primeiro você deve efetuar login como o usuário especificado como o Administrador de Aplicativo de Usuário no momento da instalação.

Para obter detalhes sobre como usar os recursos de segurança do aplicativo de usuário, consulte o Capítulo 11, “Configuração de segurança” na página 207.</td></tr>
</table>

Função	**Descrição**	**Direitos**
Gerente Organizacional	Supervisor direto de um funcionário. Cada usuário tem somente um Gerente Organizacional. **Dica:** O Gerente Organizacional pode ser considerado o gerente administrativo.	Ele tem permissão para: ◆ Ver todas as tarefas que estão nas filas do workflow de sua equipe. Esse recurso se aplica a um nível único na hierarquia de gerenciamento. Portanto, o supervisor de um Gerente Organizacional não pode ver as tarefas dos subalternos diretos desse gerente. ◆ Editar tarefas para os que a ele se reportam, exceto no caso em que um subalterno tem uma tarefa atribuída a um grupo cujo Gerente de Grupo de Tarefas não é um Gerente Organizacional. Nesse caso, o Gerente Organizacional pode ver a tarefa, mas não pode editá-la. Durante a escalação, a tarefa passa para o Gerente de Grupo de Tarefas, e não para o Gerente Organizacional. ◆ Reivindicar tarefas e cancelar a reivindicação de tarefas, além de reatribuir tarefas a membros de sua equipe. ◆ Definir relacionamentos de proxy e indicado para si e os membros de sua equipe. ◆ Ver atributos ocultos para os membros de sua equipe.

Função	Descrição	Direitos
Gerente de Grupo de Tarefas	A responsabilidade concedida a um usuário em relação a um conjunto de tarefas associadas a um grupo de tarefas. Um grupo de tarefas é uma extensão do objeto Grupo LDAP. Todo grupo de tarefas só pode ter um Gerente de Grupo de Tarefas. Os Gerentes de Grupo de Tarefas são designados pelo Administrador de Aplicativo de Usuário. Quando uma tarefa é atribuída a um grupo, o atributo srvrprvTaskManager do grupo contém o DN do usuário que é o Gerente de Grupo de Tarefas designado. Para melhor desempenho, os Gerentes de Grupo de Tarefas também são identificados por um atributo no objeto Usuário. O atributo srvprvIsTaskManager é definido como verdadeiro para um usuário que é um Gerente de Grupo de Tarefas designado.	O Gerente de Grupo de Tarefas tem permissão para: ◆ Ver e editar todas as tarefas atribuídas a um grupo para o qual ele é o líder designado. O Gerente de Grupo de Tarefas **não** tem permissão para: ◆ Criar recursos ou recolher solicitações. ◆ Definir relacionamentos de proxy e indicado. ◆ Ver atributos ocultos para os membros de sua equipe.

Observação: Todo usuário pode ver os atributos ocultos associados à sua identidade.

Definindo relacionamentos de proxy e indicado Para definir uma atribuição de proxy para um usuário, você usa a página *Atribuições de Proxy de Equipe* na guia *Solicitações e Aprovações* da interface de usuário do Identity Manager. Para definir uma atribuição de indicado para um usuário, você usa a página *Atribuições de Delegação de Equipe*, que também está disponível na guia *Solicitações e Aprovações*.

Criando Gerentes de Grupo de Tarefas Para definir um Gerente de Grupo de Tarefas para um grupo de tarefas, você usa a página *Criar Usuário ou Grupo* na guia *Auto-atendimento de Identidade* da interface de usuário do Identity Manager.

Para obter detalhes sobre como definir Gerentes de Grupo de Tarefas, proxies e delegações, consulte o *Aplicativo de Usuário do Identity Manager: Guia do Usuário*.

Configurando definições de solicitação de aprovisionamento 22

Este capítulo fornece instruções sobre como configurar as definições de solicitação de aprovisionamento. Os tópicos incluem:

22.1 Sobre o plug-in Configuração de Solicitação de Aprovisionamento

Para configurar uma definição de solicitação de aprovisionamento, é preciso usar o plug-in Configuração de Solicitação de Aprovisionamento no iManager. Esse plug-in permite que você vincule a definição de solicitação de aprovisionamento a um recurso aprovisionado, especifique as características do workflow associado e habilite-a para uso. Nesta versão, os recursos aprovisionados são mapeados para direitos do Identity Manager.

Observação: Você também pode executar definições de solicitação de aprovisionamento que são mapeados diretamente para atributos no cofre de identidade. Entretanto, os gabaritos instalados não dão suporte a esse tipo de recurso, pois eles se baseiam em direitos.

Você pode encontrar o plug-in Configuração de Solicitação de Aprovisionamento na *categoria do Identity Manager* no iManager. O plug-in inclui a *tarefa Solicitações de Aprovisionamento* na *função da Configuração de Solicitação de Aprovisionamento*. A tarefa Solicitações de Aprovisionamento consiste nestes painéis:

Painel	Descrição
Seleção de Driver de Aprovisionamento	Permite que você selecione um Driver de Aplicativo do Usuário do Identity Manager. O driver contém um conjunto de definições de solicitação de aprovisionamento pré-distribuídas, de forma que é preciso selecionar um driver antes de começar a configurar as solicitações de aprovisionamento.

Painel	Descrição
Configuração de Solicitação de Aprovisionamento	Fornece ferramentas que possibilitam: ◆ Pesquisar as definições de solicitação de aprovisionamento disponíveis e selecionar uma para configuração ◆ Criar uma nova definição de solicitação de aprovisionamento com base em uma definição existente ◆ Definir as propriedades de uma definição de solicitação de aprovisionamento ◆ Atribuir a definição de solicitação de aprovisionamento a um recurso aprovisionado ◆ Editar as configurações de destinatário e tempo de espera para cada atividade no workflow associado Quando você opta por criar uma nova solicitação de aprovisionamento ou edita uma já existente, o plug-in executa o **Assistente de Configuração de Solicitação de Aprovisionamento**.

22.2 Trabalhando com os gabaritos instalados

O Identity Manager é fornecido com um conjunto de definições de solicitações de aprovisionamento e workflows pré-distribuídos. Você pode usá-los como *gabaritos* para criar seu próprio sistema de aprovisionamento. Para configurar seu sistema, defina novos objetos com base nos gabaritos instalados e personalize esses objetos para que atendam às necessidades de sua organização.

Os gabaritos instalados permitem que você determine o número de etapas de aprovação necessárias para que a solicitação seja atendida. É possível configurar uma solicitação de aprovisionamento que requeira:

- Nenhuma aprovação
- Uma etapa de aprovação
- Duas etapas de aprovação
- Três etapas de aprovação
- Quatro etapas de aprovação
- Cinco etapas de aprovação

Você também pode especificar se deseja dar suporte a processamento seqüencial ou paralelo, e se deseja aprovar ou negar a solicitação caso ocorra tempo de espera do workflow durante o processamento.

Para obter mais informações sobre padrões de design de workflow, consulte a Seção 21.1.2, “Exemplo de aprovisionamento e workflow” na página 310.

O Identity Manager é fornecido com estes gabaritos:

Gabarito	Descrição
Aprovação de Auto-aprovisionamento	Permite que uma solicitação de aprovisionamento seja atendida sem aprovações.
Aprovação de Uma Etapa (Tempo de Espera Aprova)	Requer uma aprovação única para que a solicitação de aprovisionamento seja atendida. Se ocorrer tempo de espera de uma atividade, a atividade aprovará a solicitação e o item de trabalho será encaminhado para a próxima atividade.
Aprovação Seqüencial de Duas Etapas (Tempo de Espera Aprova)	Requer duas aprovações para que a solicitação de aprovisionamento seja atendida. Se ocorrer tempo de espera de uma atividade, a atividade aprovará a solicitação e o item de trabalho será encaminhado para a próxima atividade. Este gabarito suporta o processamento seqüencial.
Aprovação Seqüencial de Três Etapas (Tempo de Espera Aprova)	Requer três aprovações para que a solicitação de aprovisionamento seja atendida. Se ocorrer tempo de espera de uma atividade, a atividade aprovará a solicitação e o item de trabalho será encaminhado para a próxima atividade. Este gabarito suporta o processamento seqüencial.
Aprovação Seqüencial de Quatro Etapas (Tempo de Espera Aprova)	Requer quatro aprovações para que a solicitação de aprovisionamento seja atendida. Se ocorrer tempo de espera de uma atividade, a atividade aprovará a solicitação e o item de trabalho será encaminhado para a próxima atividade. Este gabarito suporta o processamento seqüencial.
Aprovação Seqüencial de Cinco Etapas (Tempo de Espera Aprova)	Requer cinco aprovações para que a solicitação de aprovisionamento seja atendida. Se ocorrer tempo de espera de uma atividade, a atividade aprovará a solicitação e o item de trabalho será encaminhado para a próxima atividade. Este gabarito suporta o processamento seqüencial.
Aprovação de Uma Etapa (Tempo de Espera Recusa)	Requer uma aprovação única para que a solicitação de aprovisionamento seja atendida. Se ocorre tempo de espera de uma atividade, o workflow recusa a solicitação. Este gabarito suporta o processamento seqüencial.
Aprovação Seqüencial de Duas Etapas (Tempo de Espera Recusa)	Requer duas aprovações para que a solicitação de aprovisionamento seja atendida. Se ocorre tempo de espera de uma atividade, o workflow recusa a solicitação. Este gabarito suporta o processamento seqüencial.

Gabarito	Descrição
Aprovação Seqüencial de Três Etapas (Tempo de Espera Recusa)	Requer três aprovações para que a solicitação de aprovisionamento seja atendida. Se ocorre tempo de espera de uma atividade, o workflow recusa a solicitação. Este gabarito suporta o processamento seqüencial.
Aprovação Seqüencial de Quatro Etapas (Tempo de Espera Recusa)	Requer quatro aprovações para que a solicitação de aprovisionamento seja atendida. Se ocorre tempo de espera de uma atividade, o workflow recusa a solicitação. Este gabarito suporta o processamento seqüencial.
Aprovação Seqüencial de Cinco Etapas (Tempo de Espera Recusa)	Requer cinco aprovações para que a solicitação de aprovisionamento seja atendida. Se ocorre tempo de espera de uma atividade, o workflow recusa a solicitação. Este gabarito suporta o processamento seqüencial.
Aprovação Paralela de Duas Etapas (Tempo de Espera Aprova)	Requer duas aprovações para que a solicitação de aprovisionamento seja atendida. Se ocorrer tempo de espera de uma atividade, a atividade aprovará a solicitação e o item de trabalho será encaminhado para a próxima atividade. Este gabarito suporta o processamento paralelo.
Aprovação Paralela de Três Etapas (Tempo de Espera Aprova)	Requer três aprovações para que a solicitação de aprovisionamento seja atendida. Se ocorrer tempo de espera de uma atividade, a atividade aprovará a solicitação e o item de trabalho será encaminhado para a próxima atividade. Este gabarito suporta o processamento paralelo.
Aprovação Paralela de Quatro Etapas (Tempo de Espera Aprova)	Requer quatro aprovações para que a solicitação de aprovisionamento seja atendida. Se ocorrer tempo de espera de uma atividade, a atividade aprovará a solicitação e o item de trabalho será encaminhado para a próxima atividade. Este gabarito suporta o processamento paralelo.
Aprovação Paralela de Cinco Etapas (Tempo de Espera Aprova)	Requer cinco aprovações para que a solicitação de aprovisionamento seja atendida. Se ocorrer tempo de espera de uma atividade, a atividade aprovará a solicitação e o item de trabalho será encaminhado para a próxima atividade. Este gabarito suporta o processamento paralelo.
Aprovação Paralela de Duas Etapas (Tempo de Espera Recusa)	Requer duas aprovações para que a solicitação de aprovisionamento seja atendida. Se ocorre tempo de espera de uma atividade, o workflow recusa a solicitação. Este gabarito suporta o processamento paralelo.

Gabarito	Descrição
Aprovação Paralela de Três Etapas (Tempo de Espera Recusa)	Requer três aprovações para que a solicitação de aprovisionamento seja atendida. Se ocorre tempo de espera de uma atividade, o workflow recusa a solicitação. Este gabarito suporta o processamento paralelo.
Aprovação Paralela de Quatro Etapas (Tempo de Espera Recusa)	Requer quatro aprovações para que a solicitação de aprovisionamento seja atendida. Se ocorre tempo de espera de uma atividade, o workflow recusa a solicitação. Este gabarito suporta o processamento paralelo.
Aprovação Paralela de Cinco Etapas (Tempo de Espera Recusa)	Requer cinco aprovações para que a solicitação de aprovisionamento seja atendida. Se ocorre tempo de espera de uma atividade, o workflow recusa a solicitação. Este gabarito suporta o processamento paralelo.

Workflows e recursos aprovisionados Cada definição de solicitação de aprovisionamento tem uma vinculação pré-configurada com um workflow e um recurso aprovisionado. Você pode mudar o recurso aprovisionado associado a uma definição de solicitação, mas não o workflow ou sua topologia.

Categorias para as solicitações de aprovisionamento Cada gabarito de solicitação de aprovisionamento também é vinculada a uma *categoria*. As categorias são uma forma conveniente de organizar as solicitações de aprovisionamento para o usuário final. A categoria padrão de todos os gabaritos de solicitação de aprovisionamento é *Direitos*. A chave de categoria, que é o valor do atributo srvprvCategoryKey, é *direitos* (letras minúsculas).

Você pode criar suas próprias categorias com o editor da camada de abstração do diretório. Ao criar uma nova categoria, certifique-se de que a chave de categoria (o valor de srvprvCategoryKey) esteja com letras minúsculas. Esse procedimento é necessário para garantir que as categorias funcionem corretamente no aplicativo de usuário do Identity Manager.

Para obter detalhes sobre como criar categorias de aprovisionamento, consulte a Seção 4.4, “Trabalhando com listas” na página 103.

22.3 Configurando uma definição de solicitação de aprovisionamento

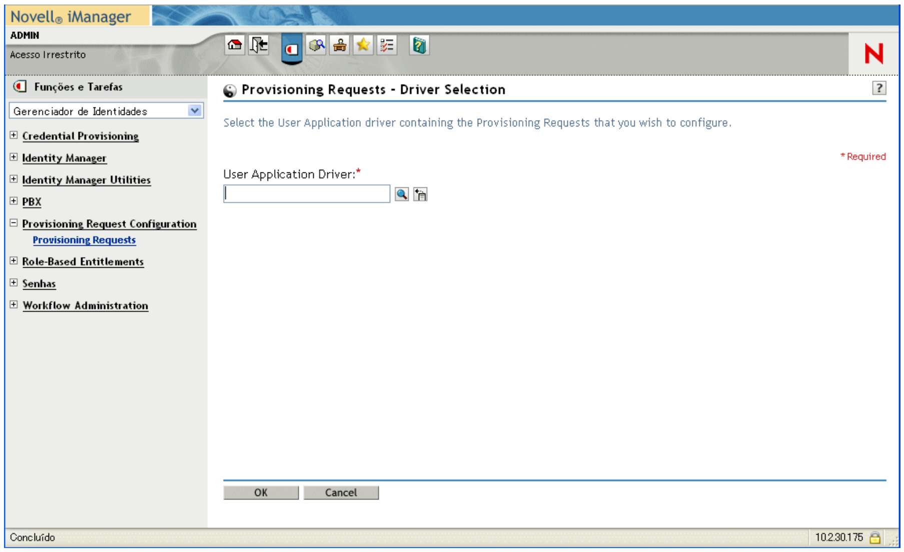
Antes de configurar uma definição de solicitação de aprovisionamento, é preciso selecionar o Driver de Aplicativo do Usuário do Identity Manager que contém a definição. Depois de selecionar o driver, você pode criar uma nova definição de solicitação de aprovisionamento ou editar uma definição existente. Você também pode apagar definições de solicitação de aprovisionamento, mudar o status de uma definição de solicitação ou estabelecer direitos para uma definição de solicitação.

22.3.1 Selecionando o driver

Para selecionar um Driver de Aplicativo do Usuário do Identity Manager:

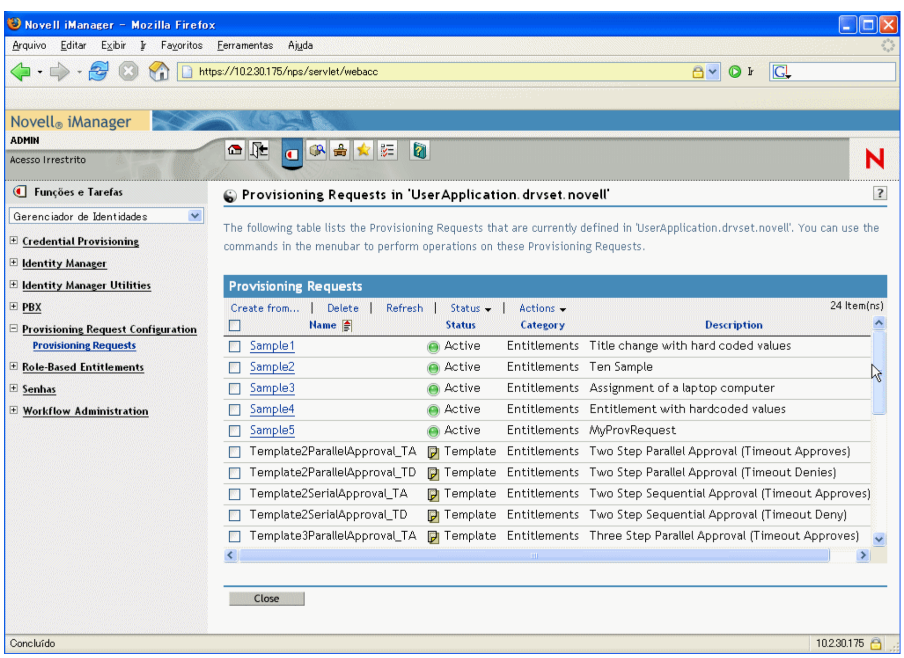
1. Selecione a categoria do *Identity Manager* no iManager.
2. Abra a função *Configuração de Solicitação de Aprovisionamento*.
3. Clique na tarefa *Solicitações de Aprovisionamento*.

   O iManager exibe a tela do Driver de Aplicativo do Usuário.



4. Especifique o nome de driver no campo *Driver de Aplicativo do Usuário* e clique em *OK*.

   O iManager exibe o painel Configuração de Solicitação de Aprovisionamento. Esse painel exibe uma lista de definições de solicitação de aprovisionamento disponíveis.



Os gabaritos instalados aparecem em um texto escuro com um status de *Gabarito*. As definições de solicitação que são gabaritos não exibem links de hipertexto, pois são apenas leitura.

Observação: Se as definições de solicitação foram configuradas para usar texto localizado, os nomes e as descrições dessas definições mostram texto adequado ao local atual.

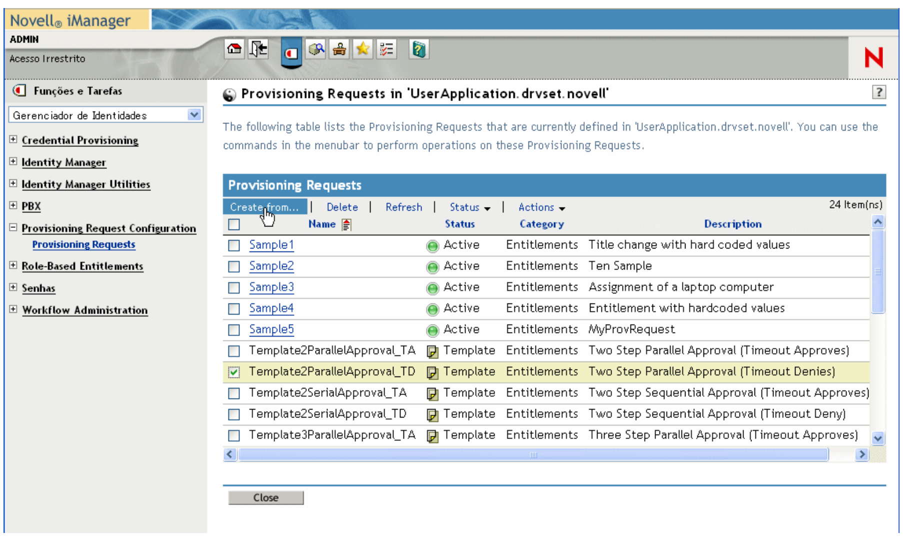
Mudando o driver Depois que você selecionar um driver, a seleção do driver permanecerá ativada durante a sessão do iManager, a não ser que você selecione um novo driver. Para selecionar um novo driver, clique no comando *Ações* e escolha *Selecionar Driver de Aplicativo do Usuário* no menu *Ações*.

22.3.2 Criando ou editando uma solicitação de aprovisionamento

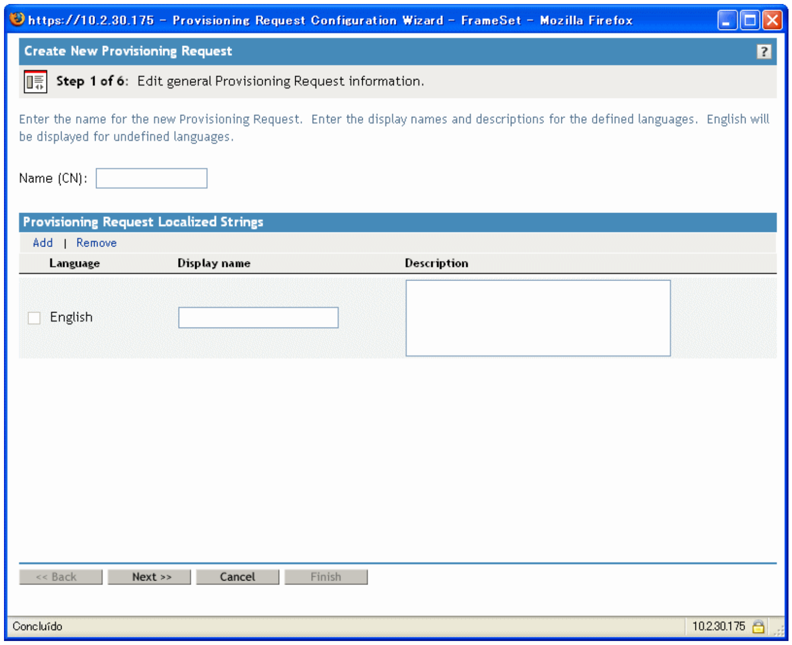
Para criar uma nova solicitação de aprovisionamento:

1 Clique no nome da solicitação de aprovisionamento que será usada como gabarito no painel Configuração de Solicitação de Aprovisionamento.

2 Clique no comando *Criar de* no painel Configuração de Solicitação de Aprovisionamento.



A primeira página do Assistente para Configurar Nova Solicitação de Aprovisionamento é exibida.



3 Digite um nome comum para o novo objeto no campo *Nome*.

4 Para cada idioma que você queira suportar em seu aplicativo, digite o texto localizado nos campos *Nome de exibição* e *Descrição* em *Strings Localizadas da Solicitação de Aprovisionamentos*. Esse texto será usado para identificar a solicitação de aprovisionamento em todo o aplicativo de usuário.

5 Para adicionar um novo idioma à lista, clique em *Adicionar* e selecione o idioma desejado.

Observação: Por padrão, uma solicitação de aprovisionamento recém-criada suporta somente o inglês.

---

6 Clique em *Avançar*.

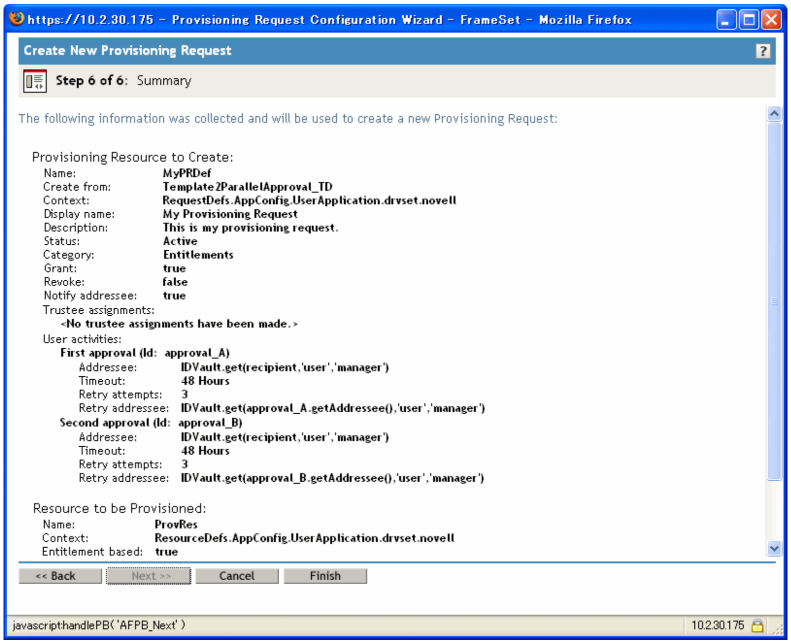
7 Especifique o recurso aprovisionado para a definição de solicitação, como descrito em "Especificando o recurso aprovisionado" na página 330.

8 Configure as atividades para o workflow associado à definição de solicitação, como descrito em "Configurando as atividades de workflow" na página 334.

9 Especifique os direitos de acesso para a definição de solicitação, como descrito em "Especificando os direitos de acesso para a solicitação de aprovisionamento" na página 338.

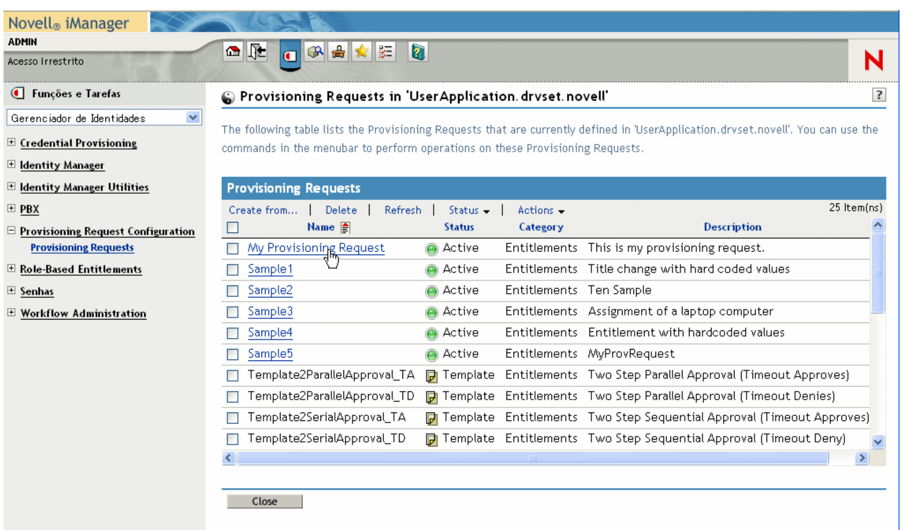
10 Especifique o status inicial para a definição de solicitação, como descrito em "Especificando o status inicial da solicitação de aprovisionamento" na página 339.

11 Verifique suas configurações e clique em *Concluir*.



Para editar uma solicitação de aprovisionamento existente:

1 Clique no nome da solicitação de aprovisionamento no painel Configuração de Solicitação de Aprovisionamento.



Você não pode editar uma solicitação de aprovisionamento que seja um gabarito. As definições de solicitação que têm um status de Gabarito não exibem links de hipertexto, pois elas são apenas leitura.

Observação: Se você tem um grande número de definições de solicitação, convém classificar a lista por uma coluna específica, como Nome ou Descrição. Para classificar por determinada coluna, basta clicar no cabeçalho da coluna.

---

2 Para cada idioma que você queira suportar em seu aplicativo, clique na caixa de seleção ao lado do idioma na lista em *Strings Localizadas da Solicitação de Aprovisionamentos* e digite o texto localizado nos campos *Nome de Exibição* e *Descrição*. Esse texto será usado para identificar a solicitação de aprovisionamento em todo o aplicativo de usuário.

3 Para adicionar um novo idioma à lista, clique em *Adicionar* e selecione o idioma desejado.

Observação: Por padrão, uma solicitação de aprovisionamento recém-criada suporta somente o inglês.

---

4 Clique em *Avançar*.

5 Especifique o recurso aprovisionado para a definição de solicitação, como descrito em "Especificando o recurso aprovisionado" na página 330.

6 Configure as atividades para o workflow associado à definição de solicitação, como descrito em "Configurando as atividades de workflow" na página 334.

7 Especifique os direitos de acesso para a definição de solicitação, como descrito em "Especificando os direitos de acesso para a solicitação de aprovisionamento" na página 338.

8 Especifique o status inicial para a definição de solicitação, como descrito em "Especificando o status inicial da solicitação de aprovisionamento" na página 339.

9 Verifique suas configurações e clique em *Concluir*.

Especificando o recurso aprovisionado

Esta seção contém instruções para a especificação de um recurso aprovisionado que se baseia em um direito. Ela não fornece informações conceituais sobre direitos ou instruções para a criação e o uso de direitos.

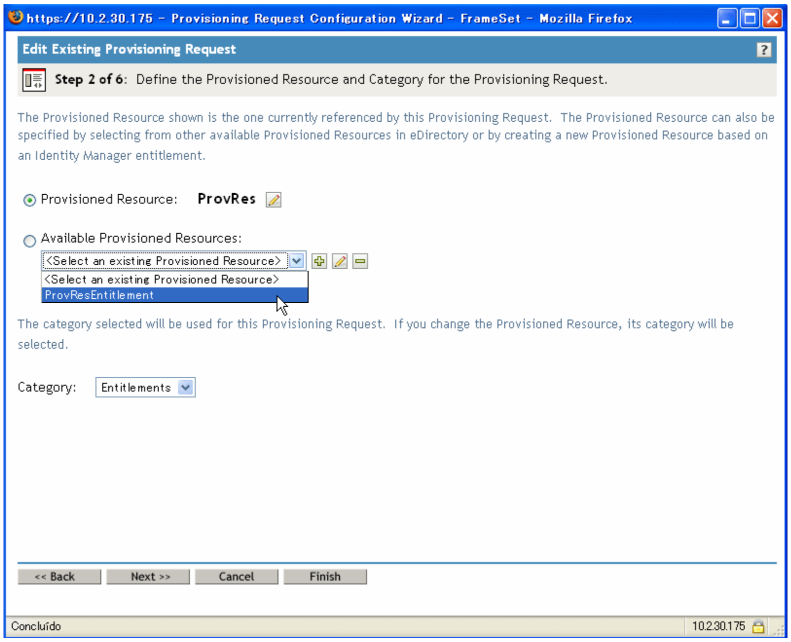
Para obter detalhes completos sobre direitos, consulte o *<z-DocTitleInVariable>Novell Identity Manager: Guia de Administração*.

Para especificar o recurso aprovisionado:

1 Para usar o destino que está associado à definição de solicitação, selecione o botão de opção *Recurso aprovisionado*.

O botão de opção Recurso aprovisionado é selecionado por padrão se você está editando uma definição de solicitação que se refere a um recurso válido. Caso você esteja redefinindo uma nova solicitação de aprovisionamento, esse botão de opção não será selecionado.

2 Para vincular a definição de solicitação a outro recurso que tenha sido previamente definido no driver selecionado, pressione o botão de opção *Recursos aprovisionados disponíveis* e selecione um destino na lista suspensa.



Observação: Se a definição de solicitação foi vinculada a um recurso que não seja um direito, você não poderá mudar o recurso.

---

3 Selecione uma categoria para a definição de recurso aprovisionado na lista suspensa *Categoria*.

A categoria padrão é a categoria do recurso aprovisionado selecionado. Sempre que você muda o recurso aprovisionado, a categoria da definição de solicitação muda para corresponder também à categoria do recurso. Se você quiser designar outra categoria à definição de solicitação, selecione essa categoria na lista suspensa Categoria.

4 Para criar um novo recurso com base em um direito do Identity Manager, clique no botão +.



Para editar um recurso existente, clique no botão em forma de caneta.



Para definir as características do recurso, siga estas etapas:

4a Especifique o nome do recurso no campo *Nome (CN)*.

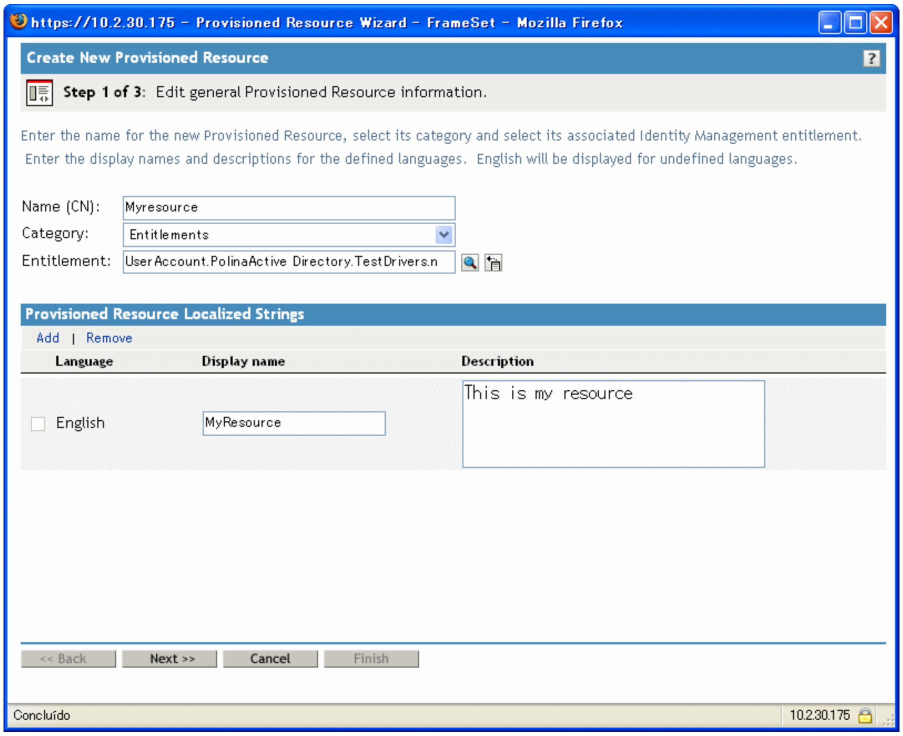
4b Selecione uma categoria para o recurso na lista suspensa *Categoria*.

4c Especifique o direito no campo *Direito*.

4d Para cada idioma que você queira suportar em seu aplicativo, clique na caixa de seleção ao lado do idioma na lista em *Strings Localizadas do Recurso Aprovisionado* e digite o texto localizado nos campos *Nome de Exibição* e *Descrição*. Esse texto será usado para identificar o recurso de aprovisionamento em todo o aplicativo de usuário.

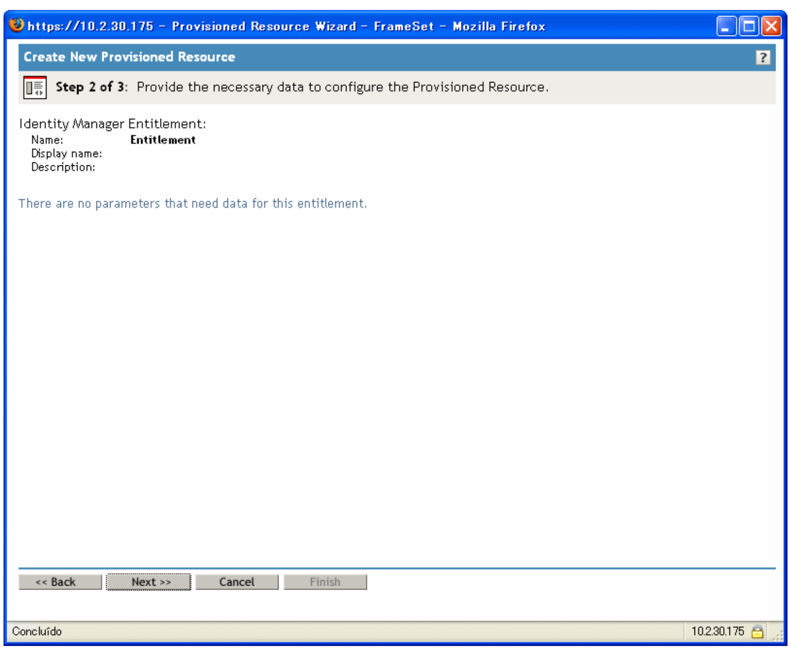
4e Para adicionar um novo idioma à lista, clique em *Adicionar* e selecione o idioma desejado.

Observação: Por padrão, um recurso de aprovisionamento recém-criado suporta somente o inglês.



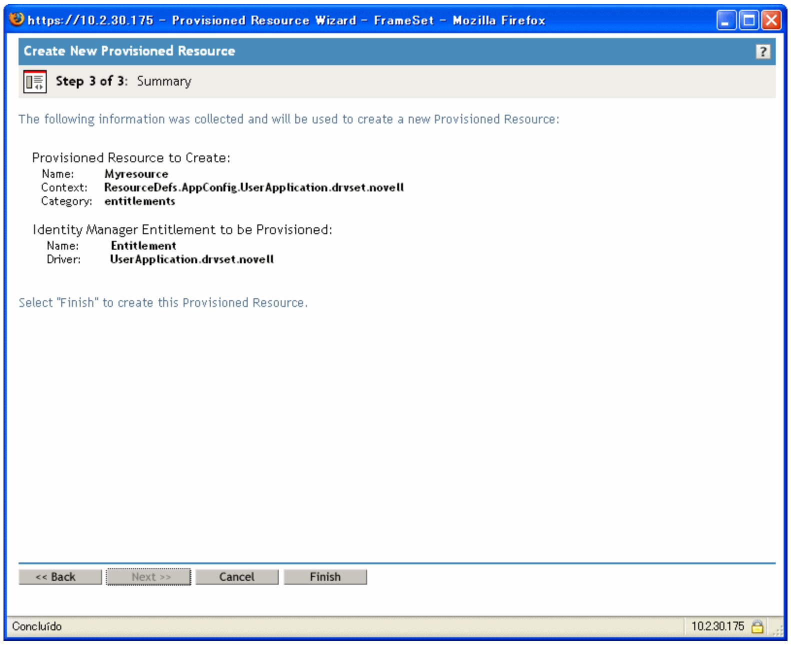
5 Clique em *Avançar*.

O Assistente de Recurso Aprovisionado exibe uma tela para que você possa fornecer dados para todos os parâmetros necessários ao direito.



6 Se o direito não exigir parâmetros de direito, clique em *Avançar*.

O assistente Criar Novo Recurso Aprovisionado exibe a página Resumo, que contém informações sobre o recurso que você está definindo.

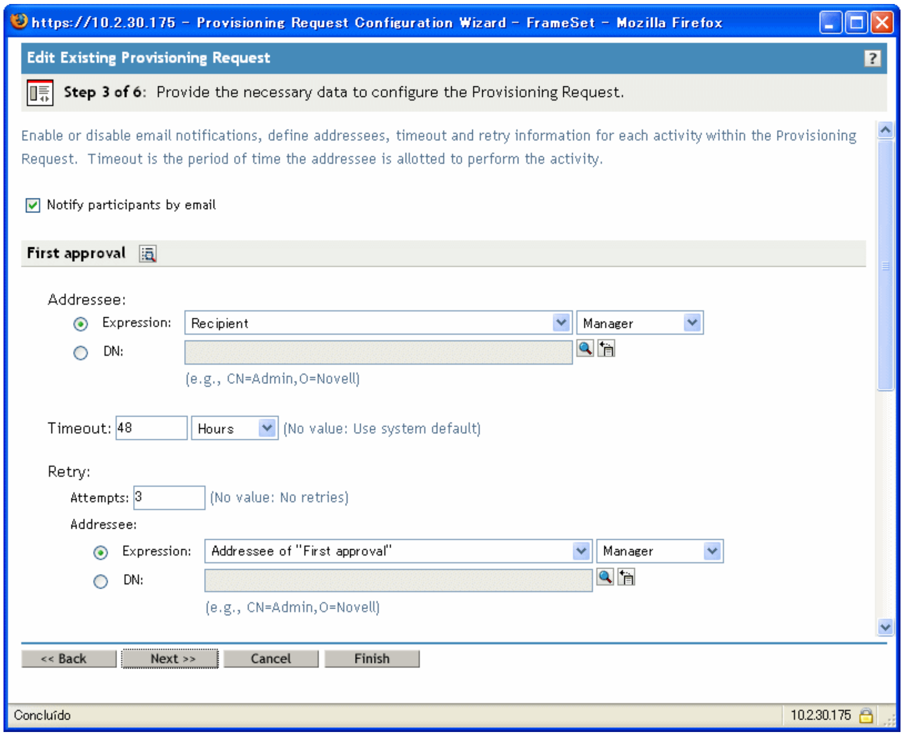


7 Clique em *Concluir*.

Configurando as atividades de workflow

Para configurar as atividades do workflow associado:

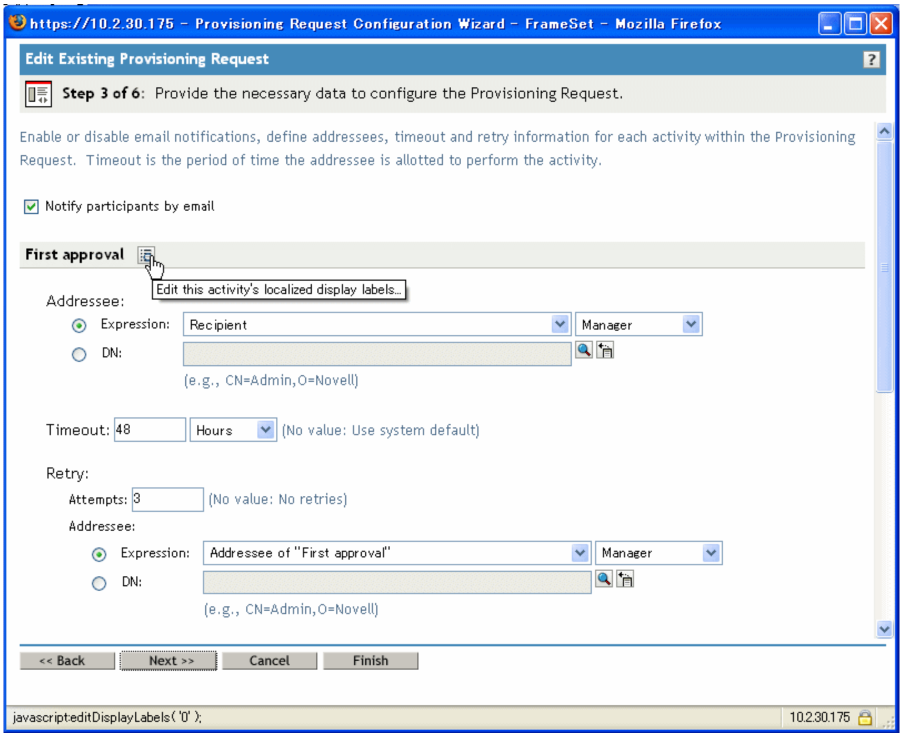
1 Marque ou desmarque a caixa de seleção *Notificar participantes por e-mail* para especificar se o destinatário de cada atividade será notificado por e-mail.



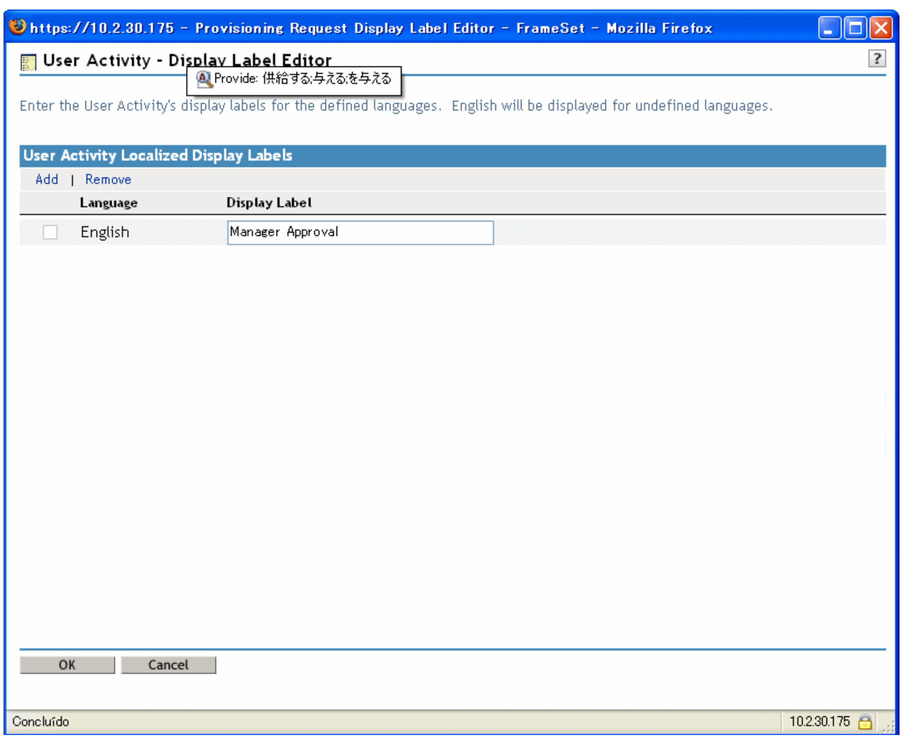
Observação: Se você marcar a caixa de seleção *Notificar participantes por e-mail* e o destinatário tiver designado um proxy, o proxy também será notificado por e-mail. Os indicados não são incluídos nas notificações por e-mail.

---

2 Para cada atividade de workflow, mude opcionalmente a etiqueta de exibição clicando no ícone ao lado no nome da atividade (nesse caso, Primeira Aprovação).



Digite a etiqueta de exibição no campo *Exibir Etiqueta* e clique em *OK*.



Observação: As etiquetas de exibição padrão (Primeira aprovação, Segunda aprovação e assim por diante) sugerem que as aprovações são processadas em seqüência. Para os fluxos paralelos, convém especificar etiquetas que não impliquem processamento seqüencial. Por exemplo, você pode atribuir etiquetas como Uma das Três Aprovações Paralelas, Duas de Três Aprovações Paralelas e assim por diante.

---

3 Para cada atividade de workflow, especifique também as seguintes informações:

Campo	Descrição
Expressão do Destinatário	Especifica uma expressão dinâmica que identifica o destinatário da atividade. O destinatário é determinado em tempo de execução, com base em como a expressão é avaliada. O **primeiro termo** da expressão de um destinatário pode ser qualquer um dos seguintes valores: ◆ `Iniciador` ◆ `Destinatário` ◆ `Destinatário de` *nome da atividade* Um termo `Destinatário de` *nome da atividade* separado é relacionado na lista suspensa Expressão de cada atividade no workflow (exceto a atividade que você está configurando). O *nome da atividade* é a etiqueta de exibição especificada para a atividade, ou o nome padrão se você não especificou uma etiqueta de exibição. O **segundo termo** da expressão de um destinatário pode ser um dos seguintes valores: ◆ `Gerenciador` ◆ `<Nenhum atributo>` **Observação:** O atributo `Gerenciador` está disponível automaticamente porque foi definido anteriormente na entidade Usuário da camada de abstração. Outros atributos (além de Gerenciador) podem estar disponíveis para seleção se atendem aos seguintes requisitos: ◆ Devem estar definidos na entidade Usuário da camada de abstração ◆ Devem ter um único valor ◆ Devem ter um tipo de dados DN
DN do Destinatário	Especifica o nome exclusivo de um usuário, grupo ou grupo de tarefas. **Observação:** Se você quiser que os Gerentes de Grupo de Tarefas possam procurar tarefas por grupo de tarefas (na ação Tarefas da Minha Equipe do aplicativo de usuário), precisará especificar o grupo de tarefas como o destinatário.

Campo	Descrição
Tempo de Espera	Especifica o período alocado para que o destinatário conclua a tarefa. O intervalo de tempo de espera se aplica toda vez que a atividade é executada pelo destinatário. Especifique um valor em segundos, minutos, horas ou dias.
Repetir Tentativas	Especifica o número de tentativas da atividade em caso de tempo de espera. Quando ocorre o tempo de espera de uma atividade, o processo de workflow pode tentar concluir a atividade novamente, dependendo do total de tentativas especificado para a atividade. Com cada tentativa, o processo de workflow pode escalar a atividade para outro usuário. Nesse caso, a atividade é reatribuída a outro destinatário (o gerente do usuário, por exemplo) para que esse usuário tenha a oportunidade de concluir o trabalho. Caso a última tentativa entre em tempo de espera, a atividade pode ser marcada como aprovada ou negada, dependendo da configuração do workflow.
Expressão do Destinatário de Repetição	Especifica uma expressão dinâmica que identifica o usuário que deve receber a tarefa caso o limite de tempo de espera seja alcançado. O destinatário de repetição é determinado em tempo de execução, com base em como a expressão é avaliada. O **primeiro termo** da expressão de um destinatário pode ser qualquer um dos seguintes valores: ◆ `approval.getAddressee()` ◆ `Iniciador` ◆ `Destinatário` ◆ `Destinatário de` *nome da atividade* A opção `approval.getAddressee()` obtém o destinatário atual. Um termo `Destinatário de` *nome da atividade* separado é relacionado na lista suspensa Expressão de cada atividade no workflow (inclusive a atividade que você está configurando). O *nome da atividade* é a etiqueta de exibição especificada para a atividade, ou o nome padrão se você não especificou uma etiqueta de exibição. O **segundo termo** da expressão de um destinatário pode ser um dos seguintes valores: ◆ `Gerenciador` ◆ `<Nenhum atributo>` Se você selecionar a opção `approval.getAddressee()` e, em seguida, selecionar `Gerenciador`, cada repetição será escalada para um novo gerente de um nível superior na organização. Portanto, você precisa assegurar que o total de repetições será um número adequado à empresa. Em todo caso, o total de repetições não deve exceder o número de níveis de gerenciamento acima do destinatário em questão.

Campo	Descrição
DN do Destinatário de Repetição	Especifica o nome exclusivo de um usuário ou grupo que deverá assumir a tarefa caso o limite de repetições seja alcançado.

4 Depois de configurar uma atividade, você talvez precise rolar a tela para ver as outras atividades do fluxo.

5 Clique em *Avançar*.

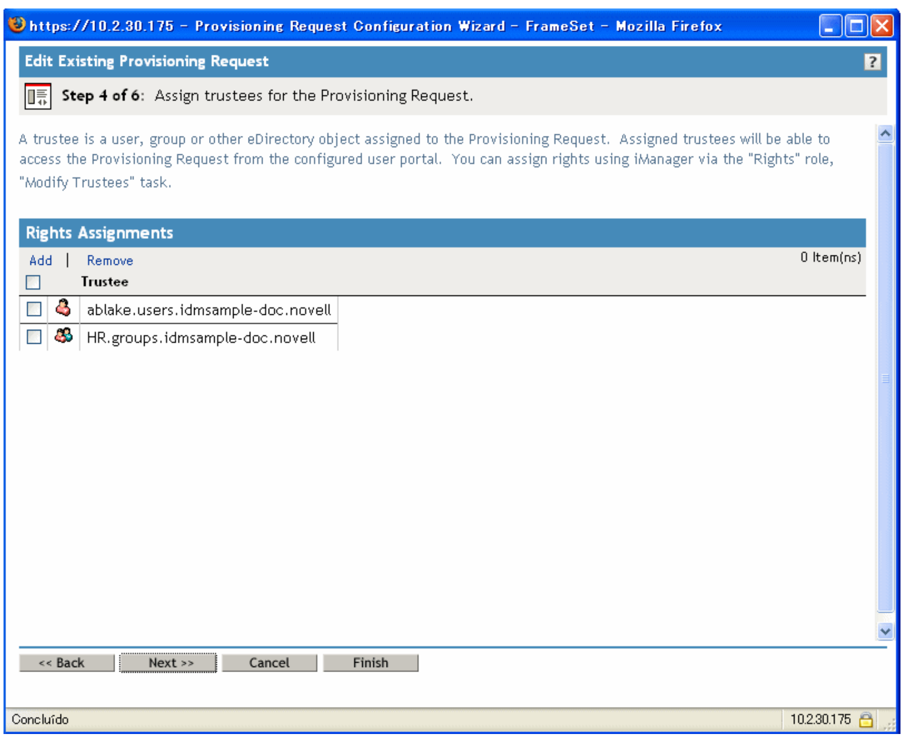
Observação: O número de atividades que podem ser configuradas varia de acordo com o gabarito de workflow que estava vinculado à definição de solicitação. O número e o tipo de parâmetros de direito varia conforme o recurso aprovisionado associado à solicitação.

Especificando os direitos de acesso para a solicitação de aprovisionamento

Para especificar os direitos de acesso de uma solicitação de aprovisionamento:

1 Para adicionar um usuário, um grupo ou outro objeto do eDirectory à lista de trustees para a definição de solicitação, clique em *Adicionar* e selecione o objeto.

Depois de adicionar um objeto, ele é incluído na lista de trustees.



2 Para remover um usuário, um grupo ou outro objeto, selecione o item na lista *Trustee* e clique em *Remover*.

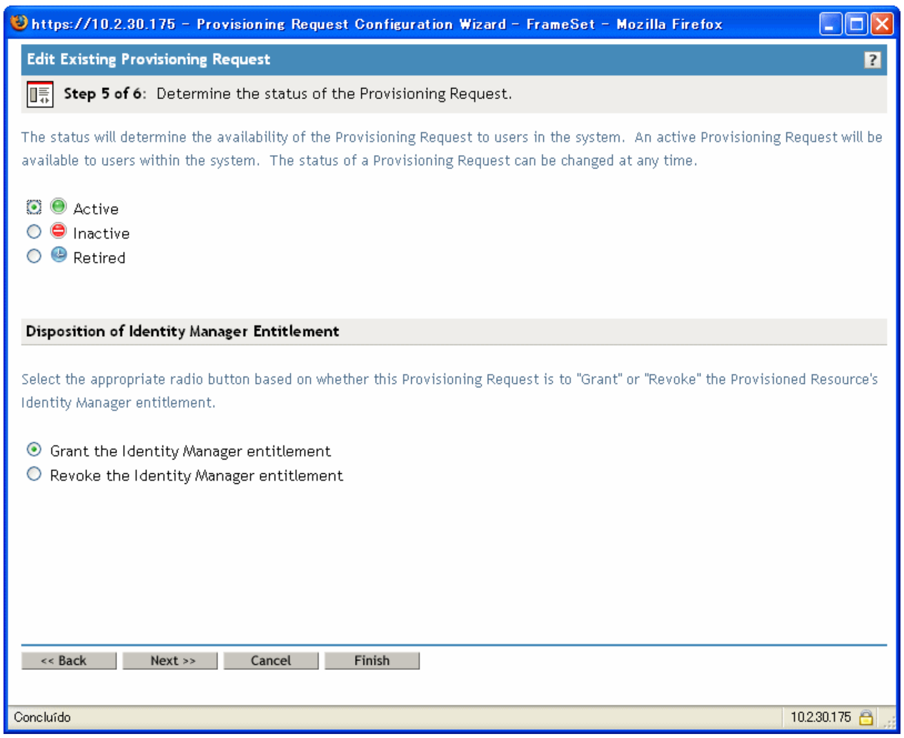
3 Clique em *Avançar*.

Especificando o status inicial da solicitação de aprovisionamento

Para definir o status inicial da solicitação de aprovisionamento:

1 Clique no botão de opção do status desejado:

Status	Descrição
Ativo	Disponível para uso.
Inativo	Temporariamente indisponível para uso. Este é o padrão.
Aposentado	Permanentemente desabilitado.



2 Clique no botão de opção da ação correta (Conceder ou Revogar).:

3 Clique em *Avançar*.

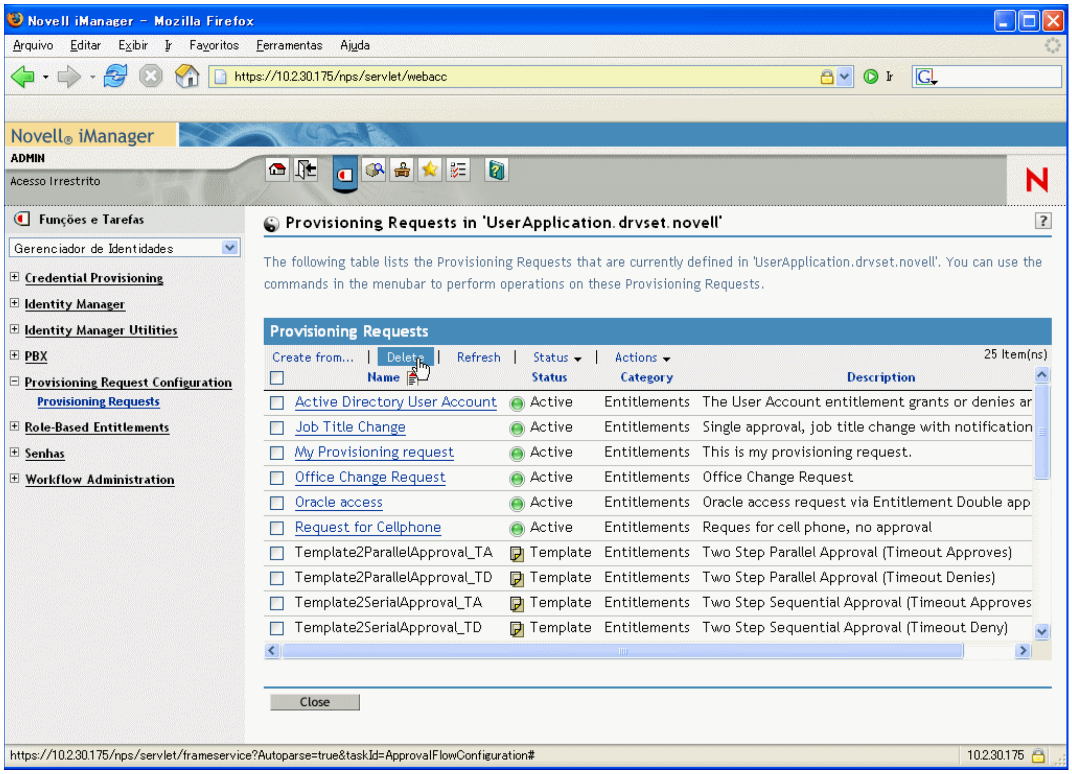
22.3.3 Apagando uma solicitação de aprovisionamento

Para apagar uma solicitação de aprovisionamento:

1 Marque a solicitação de aprovisionamento a ser apagada clicando na caixa de seleção ao lado do nome.

Você não pode apagar uma solicitação de aprovisionamento que seja um gabarito.

2 Clique no comando *Apagar* no painel Configuração de Solicitação de Aprovisionamento.

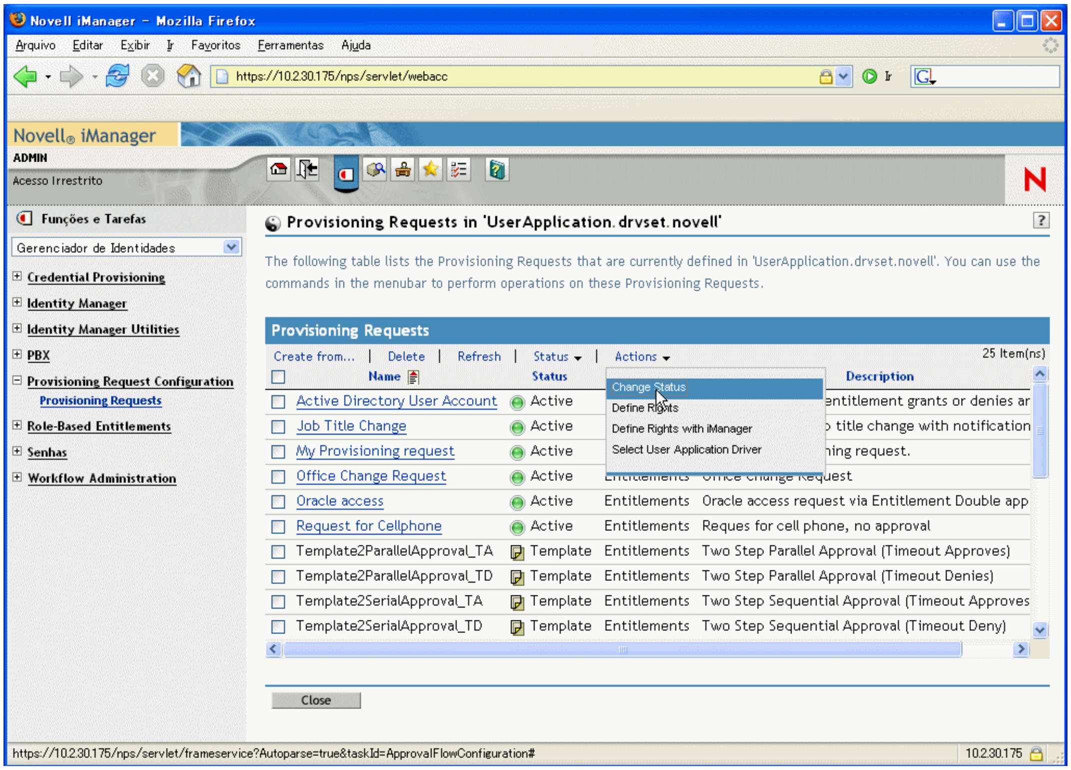


22.3.4 Mudando o status de uma solicitação de aprovisionamento existente

Para mudar o status de uma solicitação de aprovisionamento existente:

1 Marque a solicitação de aprovisionamento cujo status deve ser mudado clicando na caixa de seleção ao lado do nome.

2 Clique no comando *Mudar Status* no painel Configuração de Solicitação de Aprovisionamento.



3 Clique no status do menu Status:

Status	Descrição
Ativo	Disponível para uso.
Inativo	Temporariamente indisponível para uso.
Aposentado	Permanentemente desabilitado.

4 Clique no botão de opção da ação correta (Conceder ou Revogar).:

5 Clique em *Concluir*.

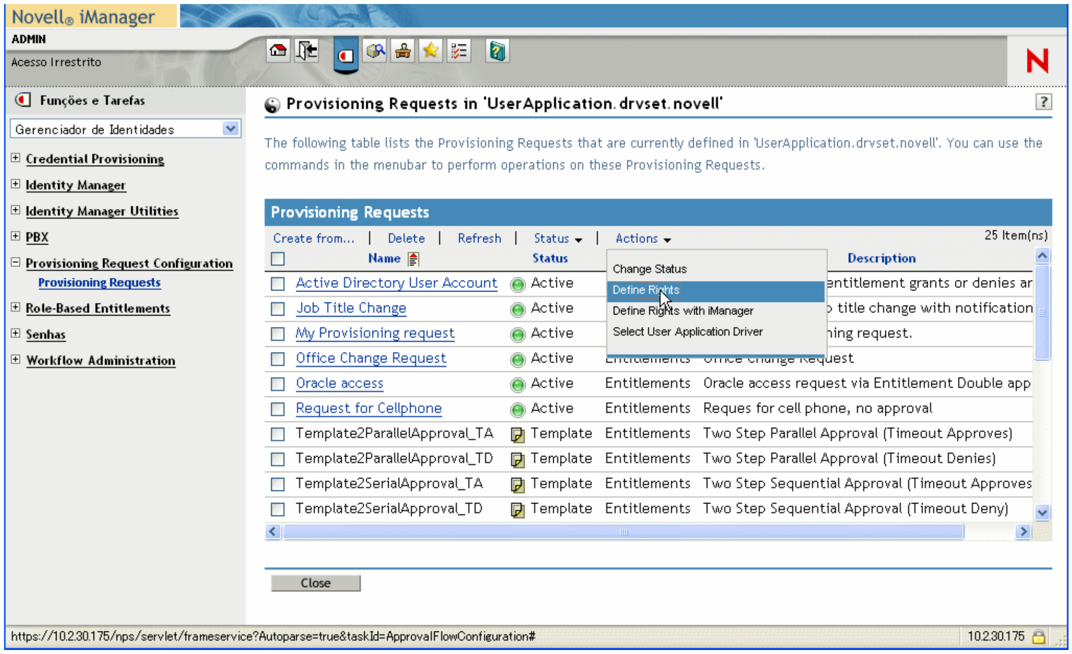
22.3.5 Definindo direitos em uma solicitação de aprovisionamento existente

Para definir direitos em uma solicitação de aprovisionamento existente:

1 Marque a solicitação de aprovisionamento para a qual você define direitos clicando na caixa de seleção ao lado do nome.

2 Clique no comando *Ações* no painel Configuração de Solicitação de Aprovisionamento.

3 Clique no comando *Definir Direitos* do menu Ações.



4 Siga as etapas apresentadas em “Especificando os direitos de acesso para a solicitação de aprovisionamento” na página 338.

Para definir direitos em uma solicitação de aprovisionamento com o iManager:

1 Marque a solicitação de aprovisionamento para a qual você deseja definir direitos clicando na caixa de seleção ao lado do nome.

2 Clique no comando *Ações* no painel Configuração de Solicitação de Aprovisionamento.

3 Clique no comando *Definir Direitos com o iManager* do menu Ações.

Gerenciando workflows de aprovisionamento

23

Este capítulo fornece instruções sobre como gerenciar workflows de aprovisionamento em tempo de execução. Ele também fornece instruções sobre como configurar notificação por e-mail para workflows de aprovisionamento.

Os tópicos incluem:

23.1 Sobre o plug-in Administração do Workflow

O plug-in Administração do Workflow para o iManager tem uma interface baseada em browser que lhe permite ver o status dos processos de workflow, redesignar atividades em um workflow ou encerrar um workflow que esteja obstruído.

Você pode encontrar o plug-in Administração do Workflow na *categoria do Identity Manager* no iManager. O plug-in inclui a *tarefa Workflows* na *função da Administração do Workflow*.

Essa função também inclui as tarefas *Gabaritos de E-mail* e *Opções do Servidor de E-mail*. As tarefas são atalhos para outras tarefas relacionadas na função *Senhas*.

Sobre a tarefa Workflows A tarefa Workflows consiste nestes painéis:

Painel	Descrição
Workflows	Fornece a principal interface de usuário para administrar workflows de aprovisionamento. A interface relaciona os workflows que estão em processamento, e permite que você execute várias ações nesses workflows. Quando você inicia a tarefa Workflows pela primeira vez, o painel Workflows requer que um Driver de Aplicativo do Usuário do Identity Manager seja selecionado. O driver aponta para um servidor de workflow. É preciso selecionar um driver para poder efetuar login no servidor e começar a administração do workflow. Depois de selecionar um driver, você poderá especificar os critérios de pesquisa para a seleção de workflows que serão gerenciados.
Detalhe do Workflow	Fornece uma interface de usuário apenas para leitura com os detalhes sobre um workflow específico.

23.2 Gerenciando workflows

Esta seção inclui procedimentos para o gerenciamento de workflows de aprovisionamento com o plug-in Administração do Workflow.

23.2.1 Conectando com um servidor de workflow

Para começar a gerenciar workflows, é preciso conectar-se a um servidor de workflow. Se o Driver de Aplicativo do Usuário estiver vinculado a um único servidor de workflow, você pode especificar o nome do driver a ser usado. Se o driver estiver associado a vários servidores de workflow, você terá que selecionar o servidor de workflow de destino.

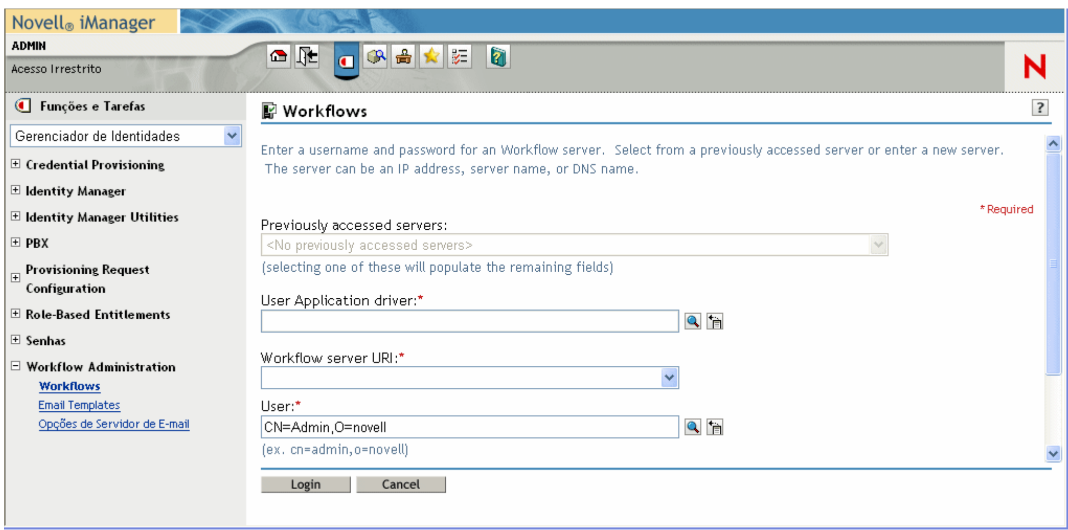
Para se conectar com um servidor de workflow:

1 Selecione a categoria do Identity Manager no iManager.

2 Abra a função *Administração do Workflow*.

3 Clique na tarefa *Workflows*.

O iManager exibe a tela Workflows.

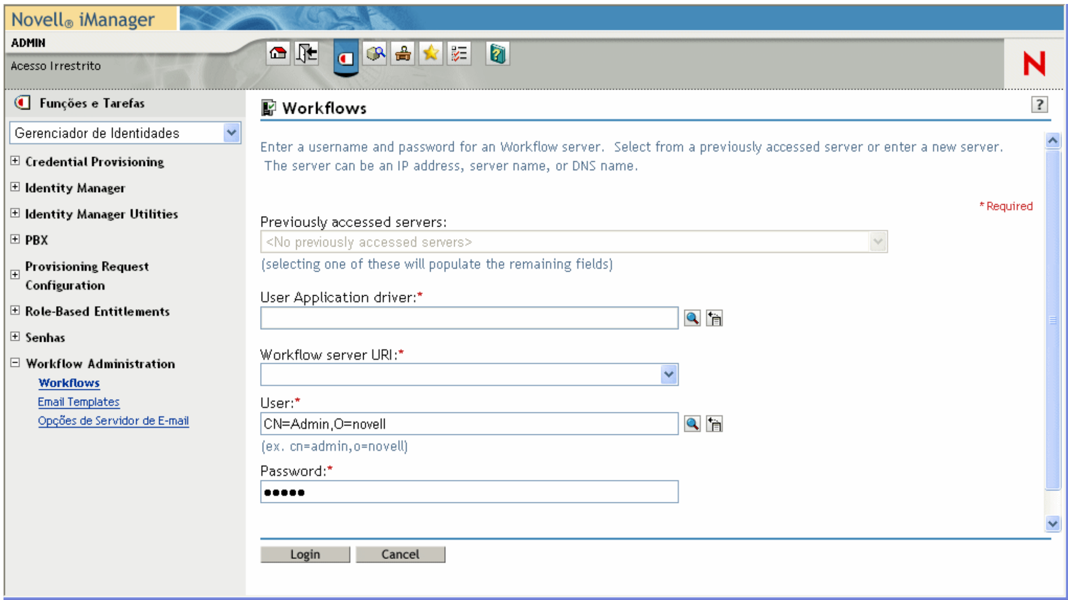


4 Se você acessou o servidor de workflow anteriormente, poderá selecionar o servidor na lista suspensa *Servidores acessados anteriormente*.

O iManager preenche os demais campos da tela.

5 Se você ainda não acessou um servidor de workflow, especifique o nome do driver no campo *Driver de Aplicativo do Usuário* e clique em *OK*.

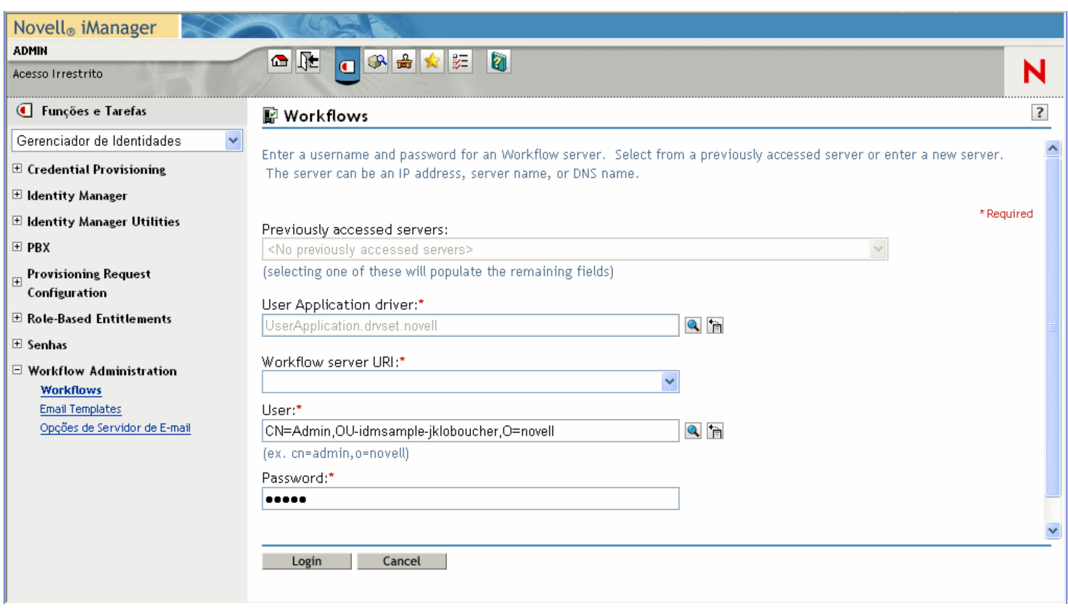
O iManager preenche os demais campos da tela.



6 Se o driver estiver associado a diversos servidores de workflow, selecione o servidor de destino no campo *URI do servidor de Workflow*.

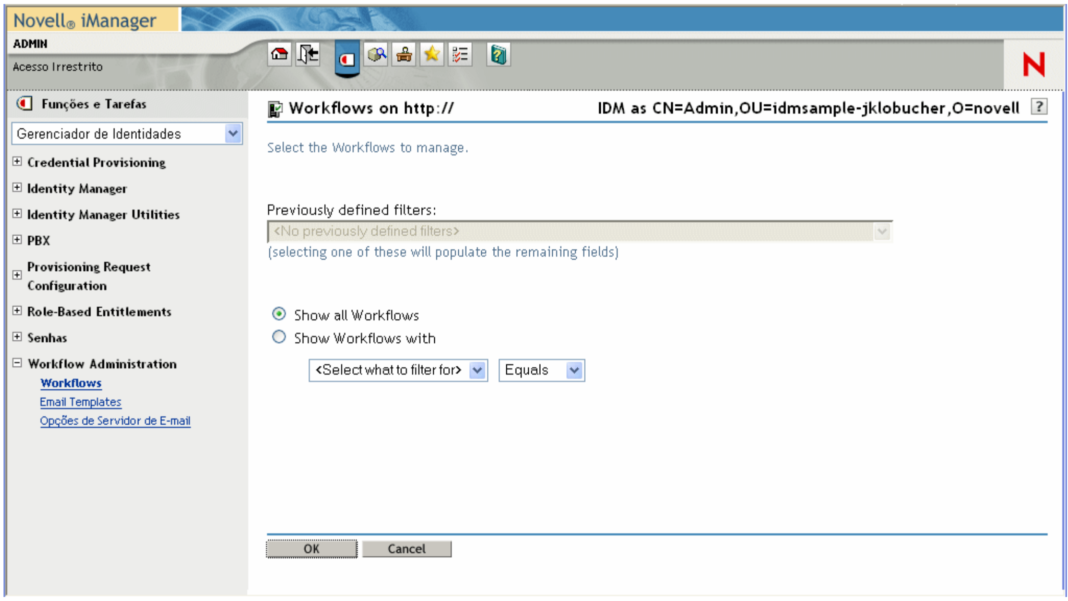
7 Opcionalmente substitua o nome de usuário no campo *Usuário* e a senha no campo *Senha*.

O usuário deve ser o Administrador de Aplicativo de Usuário. Por padrão, o nome de usuário é definido como o usuário que está conectado no iManager. Se esse usuário não for o administrador, você precisará mudar o nome de usuário. Por exemplo, você pode modificar o usuário para que aponte para o Administrador de Aplicativo de Usuário da OU de teste idmsample, como mostrado abaixo:



8 Clique em *Login*.

O plug-in Administração do Workflow exibe uma página que lhe permite especificar um filtro para localizar workflows:

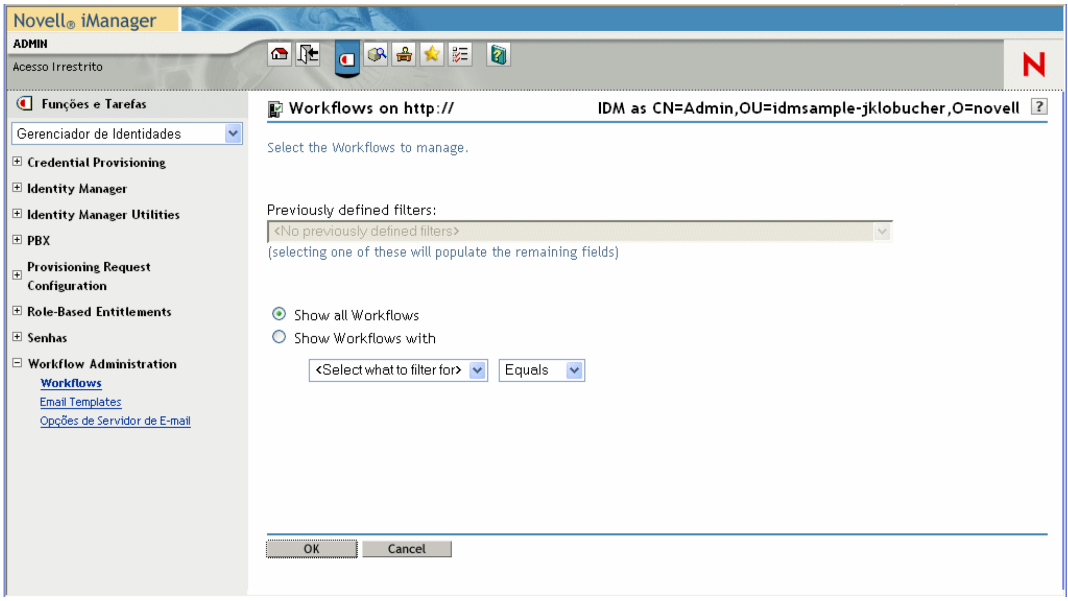


23.2.2 Localizando workflows que correspondem aos critérios de pesquisa

Se o servidor de workflow de destino executar um número elevando de processos de workflow, convém filtrar a lista de workflows exibidas no iManager. Para fazer isso, você pode especificar critérios de pesquisa.

Para especificar critérios de pesquisa para filtrar a lista de workflows:

1 Pressione o botão de opção *Mostrar Workflows com*.



Observação: Por padrão, o botão de opção *Mostrar todos os Workflows* está selecionado. Não mude o padrão se quiser ver a lista completa de workflows no servidor.

2 Selecione o atributo para o qual você deseja especificar critérios.

Atributo	Descrição
Horário de criação	Hora em que o workflow foi iniciado.
Iniciador	Nome de usuário do solicitante.
Destinatário	Nome de usuário do destinatário.
Status do Processo	Status do processo de workflow como um todo (Concluído, Executando ou Terminado).
Status da aprovação	Status do processo de aprovação (Aprovado, Negado ou Recolhido).
Status do direito	Status do direito iniciado pela solicitação de aprovisionamento (Erro, Fatal, Sucesso, Desconhecido ou Aviso).

3 Selecione um operador:

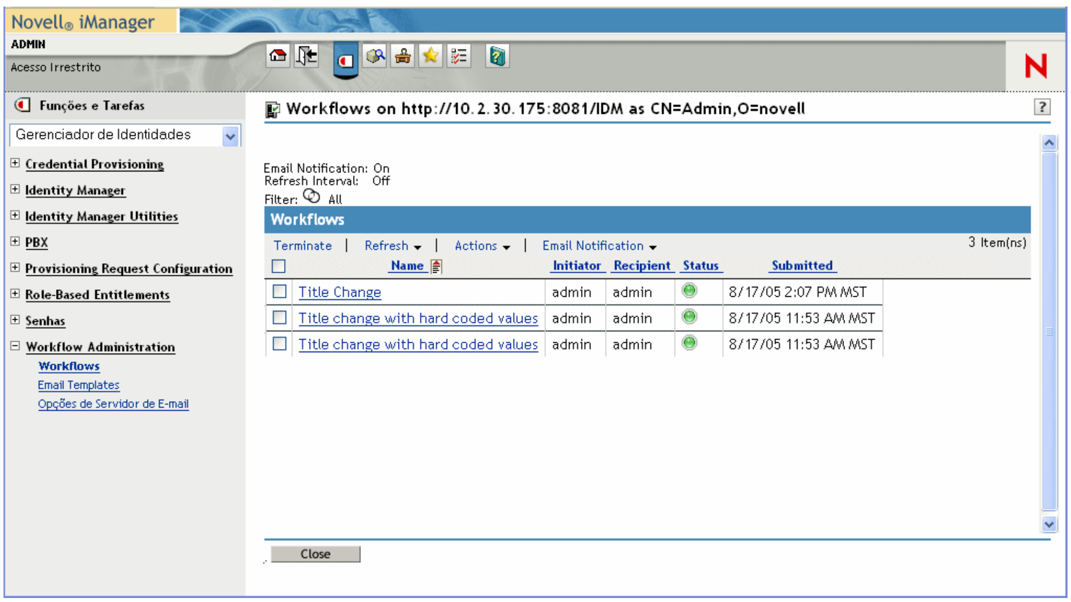
Operador	Comentário
Igual	Suportado em todos os atributos
Antes	Suportado apenas para o atributo Horário de criação.
Depois	Suportado apenas para o atributo Horário de criação.
Entre	Suportado apenas para o atributo Horário de criação.

4 Especifique um valor no campo abaixo do atributo e do operador.

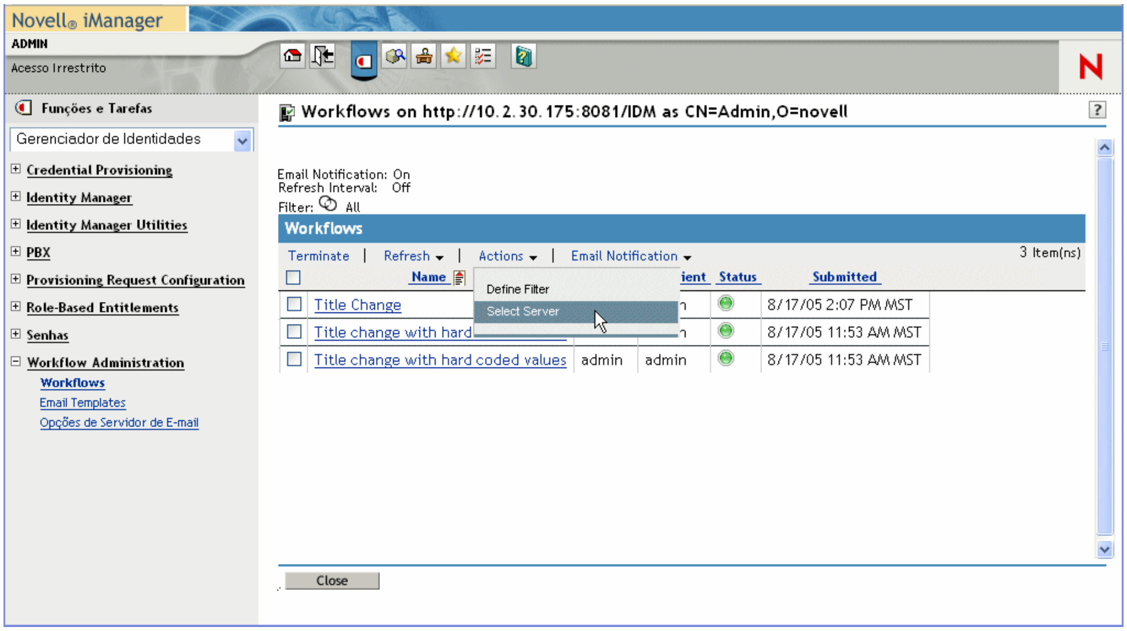
Para Horário de criação, você pode usar o controle de data e horário para selecionar o valor. Para Iniciador e Destinatário, você pode usar o Histórico do Objeto ou o Seletor de Objetos para especificar um valor. Para todos os outros atributos, selecione o valor na lista suspensa.

5 Clique em *OK*.

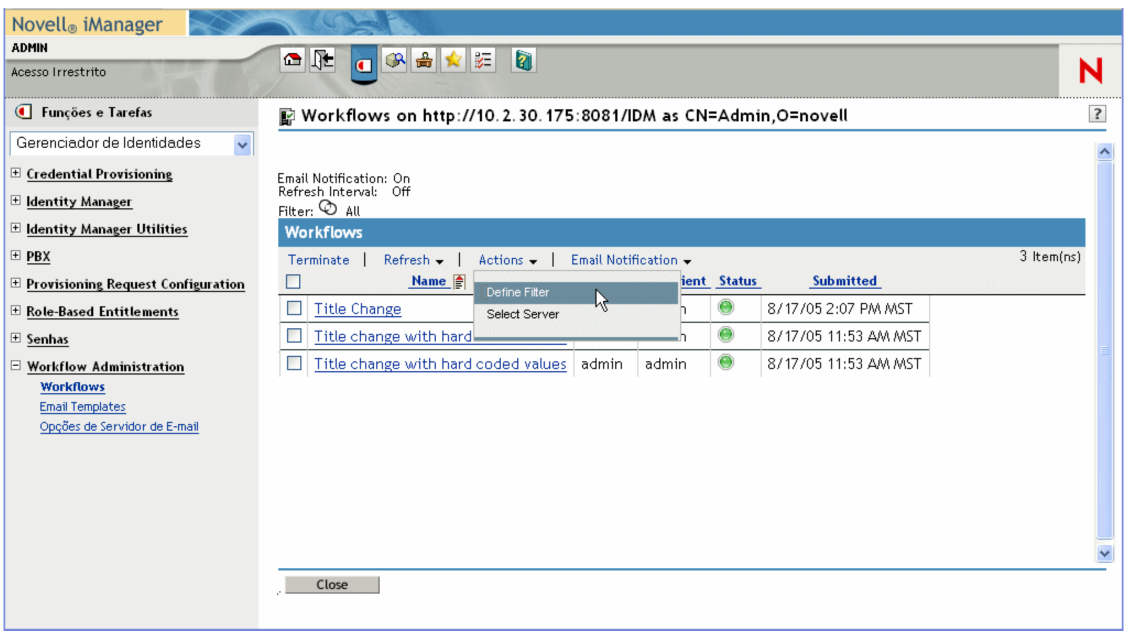
O iManager exibe os workflows que você selecionou no painel Workflows.



Mudando o servidor de destino e o filtro Depois que você selecionar um servidor de workflow, essa seleção permanecerá ativada durante a sessão do iManager, a não ser que você selecione um novo servidor. Para selecionar um novo servidor, clique no comando *Ações* e escolha *Selecionar Servidor* no menu *Ações*.



Para especificar outros critérios de pesquisa, escolha *Definir Filtro* no menu *Ações*.



23.2.3 Controlando a exibição dos workflows ativos

O painel Workflows relaciona os workflows que correspondem aos critérios de pesquisa especificados. Além de filtrar a lista, você pode controlar a exibição. Por exemplo, você pode especifica a freqüência para a atualização da lista e sua classificação em determinada coluna.

Atualizando a lista de workflows

Quando o servidor de workflow está muito ocupado, a lista de workflows ativos pode mudar constantemente. Nesse caso, convém atualizar a lista de workflows ativos em execução no servidor.

Para atualizar a lista de workflows:

1 Clique no comando *Atualizar* do painel Workflows.

2 Especifique o intervalo de atualização que será usado selecionando uma destas opções no menu Atualizar:

- **2a** Atualização Desativada
- **2b** Atualizar Agora
- **2c** 10 segundos
- **2d** 30 segundos
- **2e** 60 segundos
- **2f** 5 minutos

Classificando a lista de workflows

Se você tem um grande número de definições de solicitação, convém classificar a lista por uma coluna específica, como Nome ou Descrição.

Para classificar a lista de workflows:

1 Clique no cabeçalho da coluna de classificação.

23.2.4 Terminando uma instância de workflow

Caso você não queira que uma instância de workflow continue seu processamento, poderá terminar o workflow.

Para terminar uma instância de processo de workflow:

1 Marque o workflow no painel Workflows clicando na caixa de seleção ao lado do nome do workflow.

2 Clique no comando *Terminar* do painel Workflows.

23.2.5 Vendo detalhes sobre uma instância de workflow

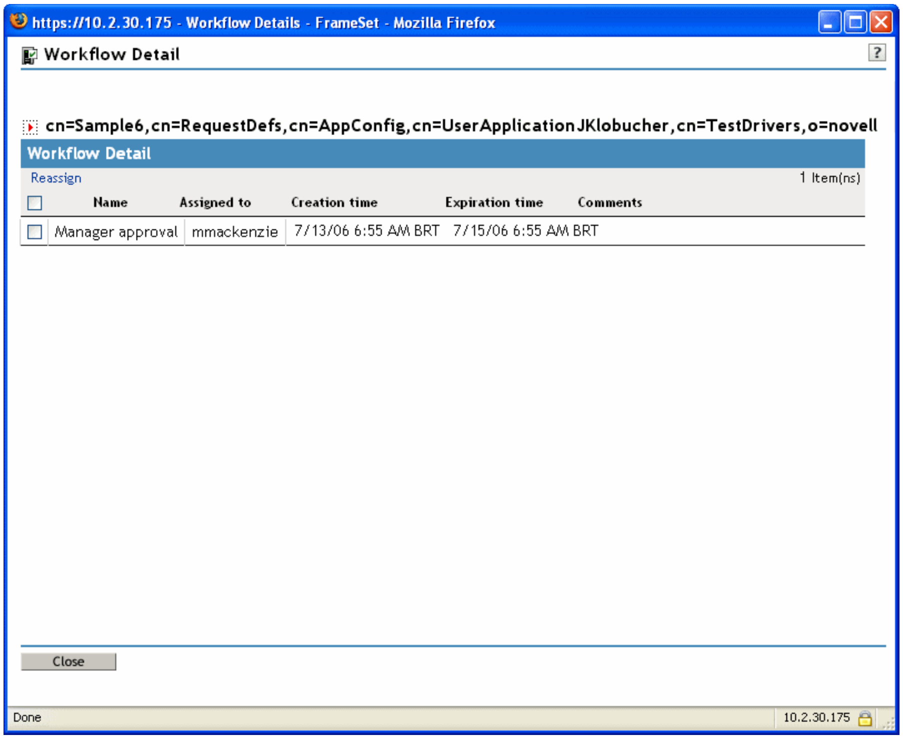
Depois de exibir um conjunto de workflows em execução em determinado servidor, você pode selecionar uma instância de workflow para ver mais detalhes sobre o processo de execução.

Observação: Se uma instância de workflow usa um padrão de design de processamento serial, a exibição mostrará uma única atividade, já que somente um usuário pode atuar no item de trabalho quando quiser. Contudo, se o workflow tratar de ramificação e processamento paralelo, pode haver várias atividades para uma instância de workflow.

Para ver detalhes sobre uma instância de workflow específica:

1 Clique no nome da instância de workflow do painel Workflows.

O iManager exibe o painel Detalhe do Workflow.



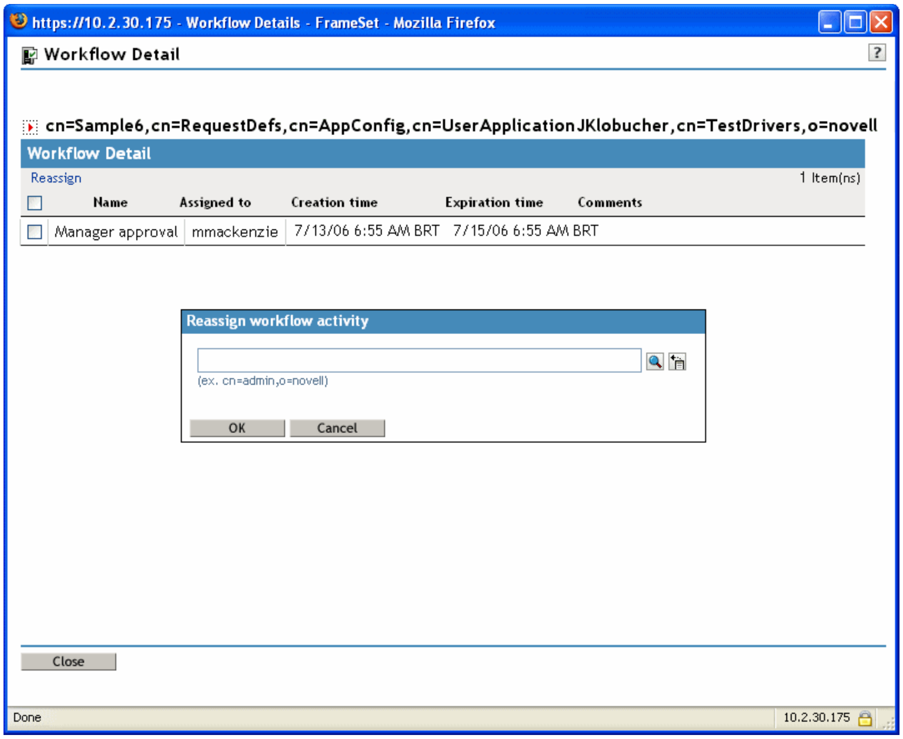
23.2.6 Reatribuindo uma instância de workflow

Caso uma instância de workflow esteja obstruída, você poderá reatribuir o item de trabalho para outro usuário ou grupo.

Para reatribuir uma instância de workflow:

1 Marque a atividade associada ao workflow clicando na caixa de seleção ao lado no nome no painel Detalhe do Workflow.

2 Clique no comando *Reatribuir* do painel Detalhe do Workflow.



3 Selecione o usuário ou o grupo ao qual você deseja reatribuir o item de trabalho.

23.3 Configurando o servidor de e-mail

Em geral, o processo de workflow envia notificações por e-mail em vários pontos durante sua execução. Por exemplo, um e-mail pode ser enviado quando um usuário atribui uma atividade de workflow a um novo destinatário.

Antes de usar os recursos de notificação por e-mail do Identity Manager, configure o servidor de e-mail SMTP. Para fazer isso, você precisa usar a tarefa *Opções do Servidor de E-mail* na função *Administração do Workflow* no iManager.

Observação: Essa tarefa é um atalho para a tarefa *Opções do Servidor de E-mail* na função *Senhas*.

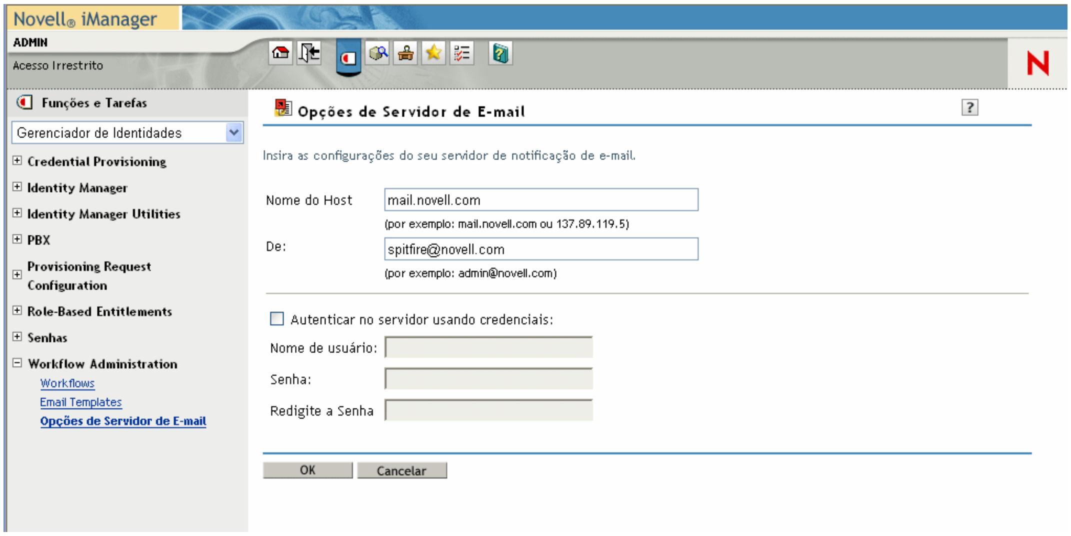
Para configurar o servidor de e-mail:

1 Selecione a categoria do Identity Manager no iManager.

2 Abra a função *Administração do Workflow*.

3 Clique na tarefa *Opções do Servidor de E-mail*.

O iManager exibe a tela Opções do Servidor de E-mail.



4 No campo *Host*, especifique o endereço IP ou o nome de host do servidor de aplicativos no qual o aplicativo de usuário é executado.

5 Digite o endereço de e-mail para o remetente no campo *De*.

Quando o destinatário abre o e-mail, esse texto é exibido no campo De do cabeçalho do e-mail. Dependendo das configurações do servidor de e-mail, o texto nesse campo pode ter que corresponder a um remetente válido no sistema para que o servidor de correio eletrônico faça pesquisas inversas ou autenticações. Um exemplo é helpdesk@company.com em vez de um texto descritivo como O Administrador de Senha.

6 Se o servidor exigir autenticação antes de enviar e-mails, marque a caixa de seleção *Autenticar no servidor com credenciais* e especifique o nome de usuário e a senha.

7 Quando terminar, clique em *OK*.

23.4 Trabalhando com o gabarito de e-mail instalado

O Identity Manager é fornecido com um gabarito de e-mail que foi elaborado especificamente para o aprovisionamento baseado em workflow. Esse gabarito de e-mail chama-se *Nova Solicitação de Aprovisionamento*. Todos os gabaritos de solicitação de aprovisionamento fornecidos com o produto são associados a esse gabarito de e-mail. Portanto, todas as novas definições de solicitação criadas usarão esse gabarito de e-mail.

Você pode editar o gabarito Nova Solicitação de Aprovisionamento para mudar o conteúdo e o formato de mensagens de e-mail. Entretanto, você não pode criar novos gabaritos de e-mail.

Para editar o gabarito Nova Solicitação de Aprovisionamento, é preciso usar a tarefa *Gabaritos de E-mail* na função *Administração do Workflow* no iManager.

Observação: Essa tarefa é um atalho para a tarefa *Editar Gabaritos de E-mail* na função *Senhas*.

23.4.1 Conteúdo e formato padrão

Esta é a aparência do gabarito Nova Solicitação de Aprovisionamento depois que você instala o produto:

```
Prezado $userFirstName$, Uma nova solicitácão de aprovisionamento foi
enviada e requer a sua aprovação. Nome da solicitação: $requestTitle$
Enviada por: $initiatorFullName$ Destinatário: $recipientFullName$
Analise os detalhes desta solicitação em $PROTOCOL$://$HOST$:$PORT$/
$TASK_DETAILS$ a fim de tomar a medida apropriada. Você pode rever uma
lista de todas as solicitações pendentes que necessitam de sua
aprovação em $PROTOCOL$://$HOST$:$PORT$/$TASKLIST_CONTEXT$.
```

O gabarito identifica a definição de solicitação de aprovisionamento que acionou a mensagem de e-mail. Ele também inclui um URL que redireciona o destinatário à tarefa que requer aprovação, bem como o URL que exibe a lista completa de tarefas pendentes do usuário.

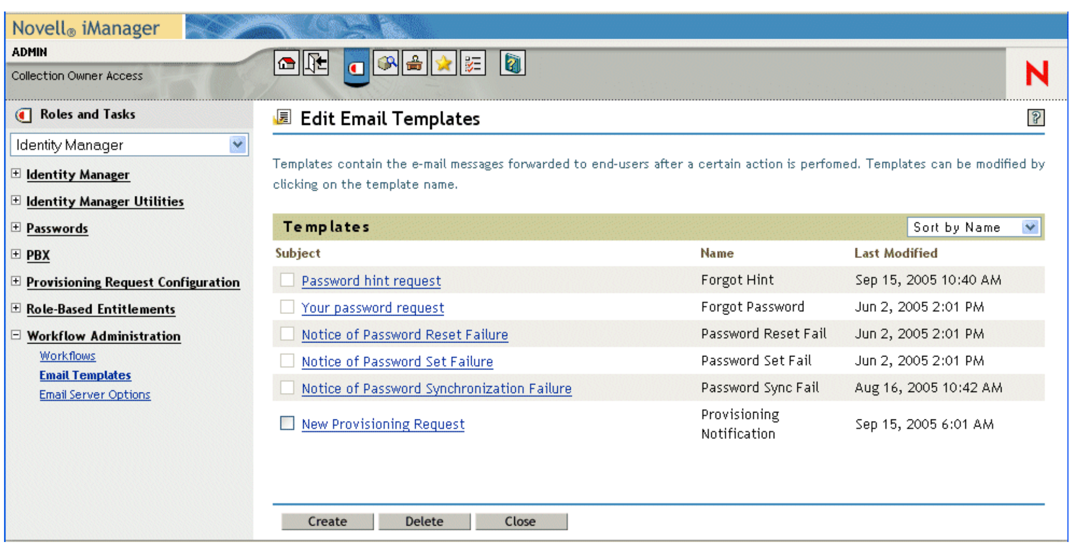
23.4.2 Editando o gabarito

Você pode mudar o conteúdo ou formatar o gabarito Nova Solicitação de Aprovisionamento. Lembre-se de que o gabarito se aplica a todas as solicitações de aprovisionamento no aplicativo de usuário do Identity Manager. Portanto, certifique-se de que suas edições sejam apropriadas para todos os usuários e tarefas de workflow.

Para editar o gabarito:

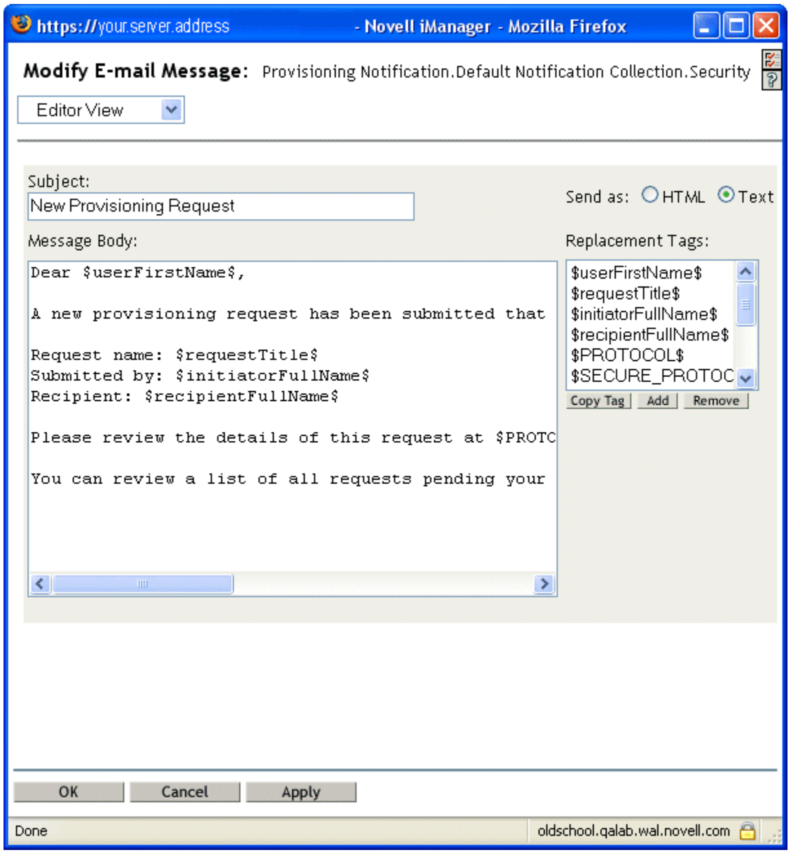
1. Selecione a categoria do Identity Manager no iManager.
2. Abra a função *Administração do Workflow*.
3. Clique na tarefa *Gabaritos de E-mail*.

   O iManager exibe a tela Editar Gabaritos de E-mail.



4 Clique em *Nova Solicitação de Aprovisionamento* na lista de gabaritos.

O iManager exibe a tela Modificar Mensagem de E-mail.



5 Efetue as mudanças na caixa *Corpo da Mensagem*.

6 Se necessário, copie uma ou mais tags da caixa de listagem Tags de Substituição para incluir texto dinâmico no corpo da mensagem.

As tags de substituição são descritas resumidamente abaixo:

Tag	Descrição
$userFirstName$	O nome do destinatário.
$requestTitle$	O nome de exibição da definição de solicitação de aprovisionamento.
$initiatorFullName$	O nome completo do iniciador.
$recipientFullName$	O nome completo do destinatário.
$PROTOCOL$	O protocolo para os URLs incluídos na mensagem de e-mail.
$SECURE_PROTOCOL$	O protocolo seguro para os URLs incluídos na mensagem de e-mail.
$HOST$	O host do servidor de aplicativos JBoss que executa o aplicativo de usuário do Identity Manager.

Tag	Descrição
$PORT$	A porta do aplicativo de usuário do Identity Manager.
$SECURE_PORT$	A porta segura do aplicativo de usuário do Identity Manager.
$TASKLIST_CONTEXT$	A página que exibe a lista de todas as solicitações pendentes para o destinatário.
$TASK_DETAILS$	A página que exibe detalhes para a solicitação para a qual a mensagem de e-mail foi gerada.

7 Quando terminar, clique em *OK*.

23.4.3 Modificando valores padrão do gabarito

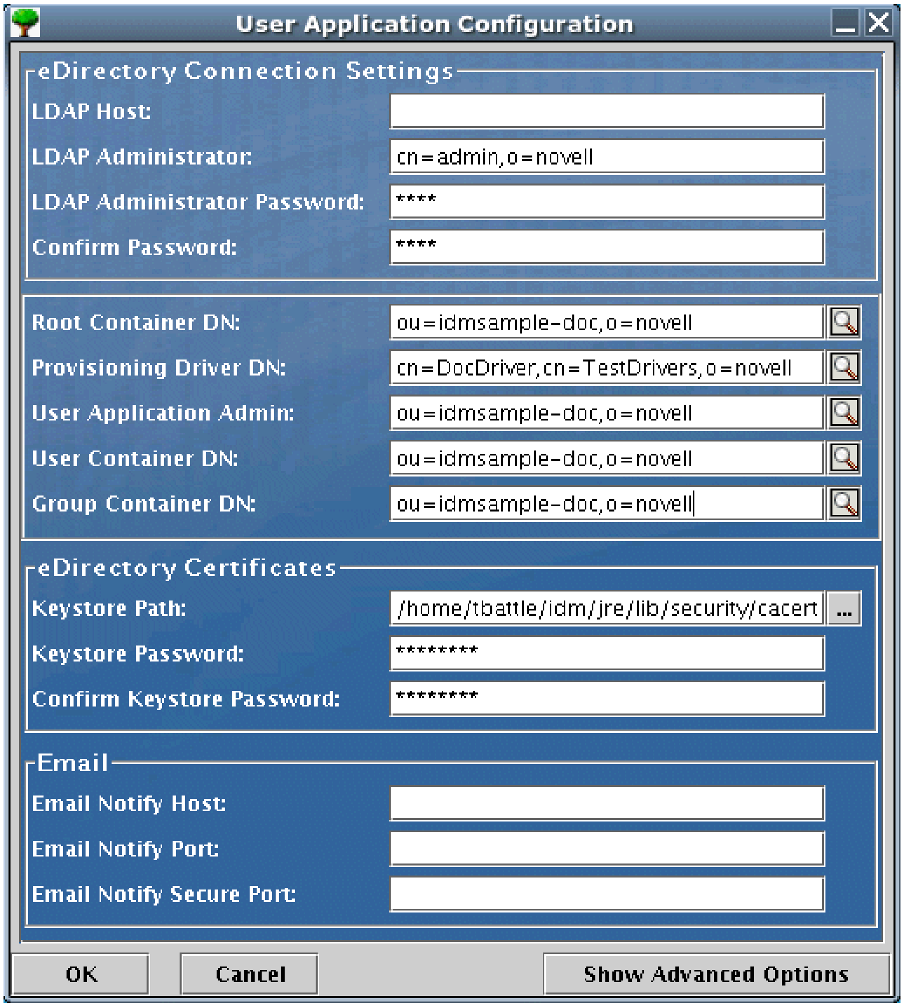
No momento da instalação, você pode definir valores padrão para diversas tags de substituição usadas nos gabaritos de e-mail. Depois que você concluir a instalação, também poderá modificar esses valores usando a ferramenta Configuração de Aplicativo de Usuário.

Para modificar as configurações de instalação

1 Execute o script ldapconfig.sh na pasta idm.

```
./configupdate.sh
```

Observação: No Windows, o arquivo a ser executado é `configupdate.bat`.



2 Faça as mudanças necessárias em qualquer um destes campos:

Campo	Descrição
Host de Notificação por E-mail	Usado para substituir o token $HOST$ em gabaritos de e-mail usados em fluxos de aprovação. Se ficar em branco, será computado pelo servidor. (Este é o host JBoss.)
Porta de Notificação por E-mail	Usado para substituir o token $PORT$ em gabaritos de e-mail usados em fluxos de aprovação.
Porta Segura de Notificação por E-mail	Usado para substituir o token $SECURE_PORT$ em gabaritos de e-mail usados em fluxos de aprovação.

3 Clique em *OK* para confirmar as mudanças.

Apêndices

VI

Os apêndices a seguir contêm informações de referência adicionais e tópicos avançados do aplicativo de usuário do Identity Manager

Extensões do esquema

A

A.1 Atribuir extensões do esquema

NOME DO ATRIBUTO	DESCRIÇÃO
srvprvAOLIMAddress	**Endereço do IM AOL**
srvprvActiveDelegatees	Os indicados ativos de um usuário
srvprvActiveDelegators	Os delegadores ativos de um usuário
srvprvAssetRef	Representação das propriedades dos valores agregados para um valor nomeado associado a um usuário por meio da classe srvprvAssetRecipientAux
srvprvAssignExpiration	Momento em que a atribuição de um proxy ou indicado expira
srvprvAssignFromContainer	Assuntos de container de uma atribuição de proxy ou indicado
srvprvAssignFromGroup	Assuntos de grupo de uma atribuição de proxy ou indicado
srvprvAssignFromUser	Assuntos de usuário de uma atribuição de proxy ou indicado
srvprvAssignToRelationship	Um relacionamento de destino de uma atribuição de indicado
srvprvAssignToUser	Os destinos do Usuário de uma atribuição de proxy ou indicado
srvprvCategoryKey	Associa determinada Definição de Solicitação de Aprovisionamento a um conjunto de categorias de aprovisionamento. Os valores são chaves para uma instância de srvprvChoice
srvprvDefaultTheme	O tema padrão
srvprvEntitlementRef	Referência a um Direito DirXML
srvprvEntityType	Especifica o tipo de definição da Entidade da Camada de Abstração do Diretório
srvprvFlowStrategy	Especifica a estratégia de chamada de fluxo a ser usada para a Definição de Solicitação de Aprovisionamento
srvprvGrant	Flag que se for verdadeira especifica que a Definição de Solicitação de Aprovisionamento tem suporte para uma operação Conceder
srvprvGroupwiseIMAddress	Endereço do IM Groupwise
srvprvHeaderFillerFile	Nome do Arquivo de Preenchimento do Cabeçalho
srvprvHeaderFillerImage	Imagem de Preenchimento do Cabeçalho
srvprvHeaderFillerLastMod	Última Modificação do Preenchimento de Cabeçalho

NOME DO ATRIBUTO	DESCRIÇÃO
srvprvAOLIMAddress	**Endereço do IM AOL**
srvprvHeaderLogo2File	Nome do Arquivo de Imagem de Logotipo Secundário de Cabeçalho
srvprvHeaderLogo2Image	Imagem de Logotipo Secundário de Cabeçalho
srvprvHeaderLogo2LastMod	Última Modificação do Logotipo Secundário de Cabeçalho
srvprvHeaderLogoFile	Nome do Arquivo de Imagem de Logotipo Primário de Cabeçalho
srvprvHeaderLogoImage	Imagem de Logotipo Secundário de Cabeçalho
srvprvHeaderLogoLastMod	Última Modificação do Logotipo Primário de Cabeçalho
srvprvHeaderTextureFile	Nome do Arquivo de Textura de Cabeçalho
srvprvHeaderTextureImage	Imagem de Textura de Cabeçalho
srvprvHeaderTextureLastMod	Última Modificação de Textura de Cabeçalho
srvprvIsTaskManager	Indica se o usuário é um gerente de grupo de tarefas
srvprvLocalizedDescrs	Fornece um conjunto de strings de descrição localizadas para os aplicativos Web de aprovisionamento, Designers e iManager
srvprvLocalizedNames	Fornece um conjunto de strings de nome de exibição para os aplicativos Web de aprovisionamento, Designers e iManager
srvprvLoginFile	Nome do Arquivo de Login
srvprvLoginImage	Imagem de Login
srvprvLoginLastMod	Última Modificação do Login
srvprvLoginSmallFile	Nome Pequeno de Arquivo de Login
srvprvLoginSmallImage	Imagem Pequena de Login
srvprvLoginSmallLastMod	Última Modificação Pequena de Login
srvprvModified	Flag para indicar mudanças em instâncias de objeto de definições no container do modelo de diretório
srvprvNavBckgrColor	Cor da Navegação em Segundo Plano
srvprvNavBckgrColorLastMod	Última Modificação da Cor de Segundo Plano de Navegação
srvprvNavColor	Cor de Navegação
srvprvNavColorLastMod	Última Modificação de Cor de Navegação
srvprvPreferredLocale	Lista de critérios de consulta/pesquisa gravados
srvprvProcessXML	Documento XML que representa uma definição de processo de aprovisionamento que inclui uma ação de workflow e aprovisionamento
srvprvRequestDefName	O nome da definição de solicitação de aprovisionamento associado a uma definição de delegação.

NOME DO ATRIBUTO	DESCRIÇÃO
srvprvAOLIMAddress	**Endereço do IM AOL**
srvprvRequestXML	Documento XML que representa o formulário de solicitação inicial e suas vinculações de dados
srvprvRevoke	Flag que se for verdadeira especifica que a Definição de Solicitação de Aprovisionamento tem suporte para uma operação Revogar
srvprvStatus	Especifica o status dos valores que o objeto de aprovisionamento suportado incluirão
srvprvTaskGroups	Grupos para os quais o usuário é um gerente de tarefas
srvprvUUID	Identificador exclusivo do portlet
srvprvTaskManager	Gerente de tarefa do grupo de tarefas
srvprvYahooIMAddress	Endereço do IM Yahoo

A.2 Extensões do esquema Objectclass

NOME DE OBJECTCLASS	DESCRIÇÃO
srvprvAppConfig	**Container para objetos Configuração de Aplicativo do Sistema de Aprovisionamento ao qual seu Driver DirXML pai se conecta**
srvprvAppDefs	Container para objetos Configuração usados para inicializar o ambiente de tempo de execução de aprovisionamento, como os temas do Portal de Identidade
srvprvAssetRecipientAux	Registra o aprovisionamento de ativos que não são de TI em um usuário
srvprvChoice	Enumeração de valores que podem ser atribuídos a determinado atributo, usados em uma consulta e assim por diante, para serem usados nos Portlets de Identidade e outros componentes do aplicativo Web
srvprvChoiceDefs	Container para as definições de Opção de Camada de Abstração do Diretório a serem expostas pelos Portlets de Identidade e os aplicativos Web
srvprvDelegateeAssignment	Definição de atribuição de indicado
srvprvDelegateeDefs	Container para definições de indicado
srvprvDirectoryModel	Container para objetos de metanível da Camada de Abstração do Diretório, conteúdo selecionado do diretório para ser exposto pelos Portlets de Identidade e os aplicativos Web
srvprvDirectoryModelConfig	Parâmetros de configuração da camada de abstração do diretório em tempo de execução
srvprvEntity	Define uma tela de atributos selecionados para classes definidas no diretório, usando Portlets de Identidade e outros componentes do aplicativo Web

NOME DE OBJECTCLASS	DESCRIÇÃO
srvprvAppConfig	**Container para objetos Configuração de Aplicativo do Sistema de Aprovisionamento ao qual seu Driver DirXML pai se conecta**
srvprvEntityAux	ObjectClass padrão
srvprvEntityDefs	Container para as definições de Entidade da Camada de Abstração do Diretório a serem expostas pelos Portlets de Identidade e os aplicativos Web
srvprvProxyAssignment	Definição de atribuição de proxy
srvprvProxyDefs	Container para definições de proxy
srvprvRelationship	Define relacionamentos entre objetos do diretório para uso nos Portlets de Identidade e outros componentes do aplicativo Web
srvprvRelationshipDefs	Container para as definições de Relacionamento da Camada de Abstração do Diretório a serem expostas pelos Portlets de Identidade e os aplicativos Web
srvprvRequest	Expõe um item de aprovisionamento a ser concedido ou revogado, incluindo o processo de workflow que define os aspectos de tempo de execução do destino de workflow e aprovisionamento
srvprvRequestDefs	Container para as definições de solicitação de aprovisionamento, o conjunto de itens que podem ser aprovisionados ao tempo de execução do aplicativo Web
srvprvResource	Define o conjunto de atribuições de diretório a ser executado para uma operação de aprovisionamento (seja Conceder ou Revogar)
srvprvResourceDefs	Container para definições de destino de aprovisionamento, incluindo descrições de tempo de design e todos os gabaritos ou destinos não utilizados
srvprvService	Descreve como chamar um Serviço Web específico em um Workflow. Isso inclui a especificação de valores de entrada e de retorno
srvprvServiceDefs	Container para objetos Definição de Serviço, que agrupam Serviços Web chamados pelos Workflows.
srvprvTaskGroupAux	Grupo de tarefas de aprovisionamento de serviço
srvprvTheme	Objeto Tema
srvprvUserAux	Entidade do usuário de aprovisionamento de serviço
srvprvWebAppConfig	Objeto Configuração de Aplicativo Web
srvprvWorkflow	Define a rede de atividades que incluem condições de impedimento a serem executadas para a obtenção de aprovação para uma ação de aprovisionamento
srvprvWorkflowDefs	Container para objetos Workflow, incluindo descrições de tempo de design e todos os gabaritos ou fluxos não utilizados
srvprvServiceDefs	Container para objetos Definição de Serviço, que agrupam Serviços Web chamados pelos Workflows.

NOME DE OBJECTCLASS	DESCRIÇÃO
srvprvAppConfig	**Container para objetos Configuração de Aplicativo do Sistema de Aprovisionamento ao qual seu Driver DirXML pai se conecta**
srvprvStatus	Especifica o status dos valores que o objeto de aprovisionamento suportado incluirão
srvprvTaskGroupAux	Grupo de tarefas de aprovisionamento de serviço
srvprvTaskGroups	Grupos para os quais o usuário é um gerente de tarefas
srvprvTaskManager	Gerente de tarefa do grupo de tarefas
srvprvTheme	Objeto Tema
srvprvUserAux	Entidade do usuário de aprovisionamento de serviço
srvprvWebAppConfig	Objeto Configuração de Aplicativo Web
srvprvWorkflow	Define a rede de atividades que incluem condições de impedimento a serem executadas para a obtenção de aprovação para uma ação de aprovisionamento
srvprvWorkflowDefs	Container para objetos Workflow, incluindo descrições de tempo de design e todos os gabaritos ou fluxos não utilizados
srvprvYahooIMAddress	Endereço do IM Yahoo

A.3 Representação LDIF

As informações completas sobre esquema que incluem sintaxes, regras de contenção e outras não exibidas nas tabelas de resumo anteriores são fornecidas abaixo (em formato LDIF). Essas informações estão sujeitas a mudanças.

```
versão: 1 # Copyright (c) 2004-2005 Trabalho Não Publicado da Novell,
Inc. Todos os Direitos # Reservados. # # ESTE É UM TRABALHO NÃO
PUBLICADO E CONTÉM INFORMAÇÕES CONFIDENCIAIS, # PROPRIETÁRIAS E DE
SEGREDO COMERCIAL DA NOVELL, INC. O ACESSO A # ESTE TRABALHO ESTÁ
RESTRITO A (I) OS FUNCIONÁRIOS DA NOVELL, INC. QUE PRECISEM # SABER
COMO EXECUTAR TAREFAS REFERENTES A SUAS ATRIBUIÇÕES E # (II) ENTIDADES
ALÉM DA NOVELL, INC. QUE TENHAM ESTABELECIDO # CONTRATOS DE LICENÇA
APROPRIADOS. NENHUMA PARTE DESTE TRABALHO PODE SER USADA, # PRATICADA,
EXECUTADA, COPIADA, DISTRIBUÍDA, REVISADA, MODIFICADA, #  TRADUZIDA,
ABREVIADA, CONDENSADA, EXPANDIDA, COLETADA, COMPILADA, #  VINCULADA,
REMODELADA, TRANSFORMADA OU ADAPTADA SEM O CONSENTIMENTO PRÉVIO #  POR
ESCRITO DA NOVELL, INC. TODO USO OU EXPLORAÇÃO DESTE TRABALHO SEM #
AUTORIZAÇÃO PODE SUJEITAR O INFRATOR A PENALIDADES CRIMINAIS E #
CIVIS. # # Base schema extensions for SpitFire # # Last Modified: 6/27/
05 (ek) # # See rfc2252 for information on attribute syntax definitions
#   String = 1.3.6.1.4.1.1466.115.121.1.15 #   Boolean =
1.3.6.1.4.1.1466.115.121.1.7 #   Octet String =
1.3.6.1.4.1.1466.115.121.1.40 #  DN = 1.3.6.1.4.1.1466.115.121.1.12 #
Case Exact String = 1.3.6.1.4.1.1466.115.121.1.26 #   Case Ignore List
= 2.16.840.1.113719.1.1.5.1.6 #   Case Ignore String =
1.3.6.1.4.1.1466.115.121.1.15 #   Stream =
```

```
1.3.6.1.4.1.1466.115.121.1.5 #   Time = 1.3.6.1.4.1.1466.115.121.1.24
# # OID registered for EPM: #   subarc "450" registered at: https://
wiki.innerweb.novell.com/wiki.phtml?title=OID_Registration #
attribute prefix: 2.16.840.1.113719.1.450.4.{3 digit unique per
attribute} #   object class prefix: 2.16.840.1.113719.1.450.6.{3 digit
unique number per class} #------------------------------------------
--------------------------------------------------------------------
---------- #-- Framework Attributes #-------------------------------
--------------------------------------------------------------------
--------------------- dn: cn=schema changetype: modify add:
attributeTypes attributeTypes: ( 2.16.840.1.113719.1.450.4.127 NAME
'srvprvUUID' DESC 'Standard Attribute' SYNTAX
1.3.6.1.4.1.1466.115.121.1.26{64512} SINGLE-VALUE X-NDS_PUBLIC_READ
'1' X-NDS_NOT_SCHED_SYNC_IMMEDIATE '1' ) dn: cn=schema changetype:
modify add: objectClasses objectClasses: (
2.16.840.1.113719.1.450.6.127 NAME 'srvprvEntityAux' DESC 'Standard
ObjectClass' AUXILIARY MAY srvprvUUID X-NDS_NOT_CONTAINER '1' ) #-----
--------------------------------------------------------------------
-------------------------------------------------- #-- User Attributes
#-------------------------------------------------------------------
-------------------------------------------------------- dn: cn=schema
changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.60 NAME 'srvprvHideUser' DESC 'Indicates if
a user is hidden during searches' SYNTAX 1.3.6.1.4.1.1466.115.121.1.7
SINGLE-VALUE ) dn: cn=schema changetype: modify add: attributeTypes
attributeTypes: ( 2.16.840.1.113719.1.450.4.61 NAME
'srvprvHideAttributes' DESC 'List of attributes a user is hiding from
other users' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 ) dn: cn=schema
changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.62 NAME 'srvprvQueryList' DESC 'List of
saved query/search criteria' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE ) dn: cn=schema changetype: modify add: attributeTypes
attributeTypes: ( 2.16.840.1.113719.1.450.4.63 NAME
'srvprvCapabilities1' DESC 'Place holder for classifying skills,
knowledge, references, etc.  Classifications are defined in the
application.' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 ) dn: cn=schema
changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.64 NAME 'srvprvCapabilities2' DESC 'Place
holder for classifying skills, knowledge, references, etc.
Classifications are defined in the application.' SYNTAX
1.3.6.1.4.1.1466.115.121.1.15 ) dn: cn=schema changetype: modify add:
attributeTypes attributeTypes: ( 2.16.840.1.113719.1.450.4.65 NAME
'srvprvCapabilities3' DESC 'Place holder for classifying skills,
knowledge, references, etc.  Classifications are defined in the
application.' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 ) dn: cn=schema
changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.66 NAME 'srvprvCapabilities4' DESC 'Place
holder for classifying skills, knowledge, references, etc.
Classifications are defined in the application.' SYNTAX
1.3.6.1.4.1.1466.115.121.1.15 ) dn: cn=schema changetype: modify add:
attributeTypes attributeTypes: ( 2.16.840.1.113719.1.450.4.67 NAME
'srvprvCapabilities5' DESC 'Place holder for classifying skills,
knowledge, references, etc.  Classifications are defined in the
application.' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 ) dn: cn=schema
```

```
changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.68 NAME 'srvprvIMAddress' DESC 'Key-value
pair of Instant messenger Addresses i.e. groupwise~jsmith' SYNTAX
1.3.6.1.4.1.1466.115.121.1.15 ) # This is temporary until we convert
the application to use the multi-value IM address (srvprvIMAddress)
above dn: cn=schema changetype: modify add: attributeTypes
attributeTypes: ( 2.16.840.1.113719.1.450.4.69 NAME
'srvprvGroupwiseIMAddress' DESC 'Groupwise IM address' SYNTAX
1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE ) # This is temporary until
we convert the application to use the multi-value IM address
(srvprvIMAddress) above dn: cn=schema changetype: modify add:
attributeTypes attributeTypes: ( 2.16.840.1.113719.1.450.4.70 NAME
'srvprvYahooIMAddress' DESC 'Yahoo IM address' SYNTAX
1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE ) # This is temporary until
we convert the application to use the multi-value IM address
(srvprvIMAddress) above dn: cn=schema changetype: modify add:
attributeTypes attributeTypes: ( 2.16.840.1.113719.1.450.4.71 NAME
'srvprvAOLIMAddress' DESC 'AOL IM address' SYNTAX
1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE ) dn: cn=schema changetype:
modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.72 NAME 'srvprvActiveDelegatees' DESC 'The
active delegatees of a user' SYNTAX  2.16.840.1.113719.1.1.5.1.6 ) dn:
cn=schema changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.73 NAME 'srvprvActiveDelegators' DESC 'The
active delegators of a user' SYNTAX  2.16.840.1.113719.1.1.5.1.6 ) dn:
cn=schema changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.74 NAME 'srvprvIsTaskManager' DESC
'Indicates if user is a task group manager' SYNTAX
1.3.6.1.4.1.1466.115.121.1.7 SINGLE-VALUE ) dn: cn=schema changetype:
modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.75 NAME 'srvprvTaskGroups' DESC 'Groups for
which the user is a task manager' SYNTAX
1.3.6.1.4.1.1466.115.121.1.12 ) dn: cn=schema changetype: modify add:
attributeTypes attributeTypes: ( 2.16.840.1.113719.1.450.4.77 NAME
'srvprvPreferredLocale' DESC 'List of saved query/search criteria'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE ) dn: cn=schema
changetype: modify add: objectclasses objectClasses: (
2.16.840.1.113719.1.450.6.128 NAME 'srvprvUserAux' DESC 'Service
provisioning user entity' AUXILIARY MAY ( srvprvHideUser $
srvprvHideAttributes $ srvprvQueryList $ srvprvCapabilities1 $
srvprvCapabilities2 $ srvprvCapabilities3 $ srvprvCapabilities4 $
srvprvCapabilities5 $ srvprvIMAddress $ srvprvGroupwiseIMAddress $
srvprvYahooIMAddress $  srvprvAOLIMAddress $ srvprvIsTaskManager $
srvprvTaskGroups $ srvprvActiveDelegatees $ srvprvActiveDelegators $
srvprvPreferredLocale) X-NDS_NOT_CONTAINER '1' ) dn: cn=schema
changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.129 NAME 'srvprvTaskManager' DESC 'Task
manager of the task group' SYNTAX  1.3.6.1.4.1.1466.115.121.1.12 ) dn:
cn=schema changetype: modify add: objectclasses objectClasses: (
2.16.840.1.113719.1.450.6.130 NAME 'srvprvTaskGroupAux' DESC 'Service
provisioning task group' AUXILIARY MAY ( srvprvTaskManager ) X-
NDS_NOT_CONTAINER '1' ) #-------------------------------------------
----------------------------------------------------------------------
--------- #-- Provisioning Attributes #-------------------------------
```

```
-----------------------------------------------------------------------
----------------------- dn: cn=schema changetype: modify add:
attributeTypes attributeTypes: ( 2.16.840.1.113719.1.450.4.100 NAME
'srvprvCategoryKey' DESC 'Associates a given Provisioning Request
Definition to a set of provisioning categories. Values are keys to a
srvprvChoice instance.' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 ) dn:
cn=schema changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.101 NAME 'srvprvGrant' DESC 'Flag which if
true specifies that the Provisioning Request Definition supports a
Grant operation.' SYNTAX 1.3.6.1.4.1.1466.115.121.1.7 SINGLE-VALUE )
dn: cn=schema changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.102 NAME 'srvprvRevoke' DESC 'Flag which if
true specifies that the Provisioning Request Definition supports a
Revoke operation.' SYNTAX 1.3.6.1.4.1.1466.115.121.1.7 SINGLE-VALUE )
dn: cn=schema changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.103 NAME 'srvprvFlowStrategy' DESC
'Specifies the flow invocation strategy to be used for the Provisioning
Request Definition.' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE
) dn: cn=schema changetype: modify add: attributeTypes attributeTypes:
( 2.16.840.1.113719.1.450.4.104 NAME 'srvprvLocalizedNames' DESC
'Provides set of localized display name strings for the provisioning
web applications, Designers and iManager.' SYNTAX
1.3.6.1.4.1.1466.115.121.1.26 ) dn: cn=schema changetype: modify add:
attributeTypes attributeTypes: ( 2.16.840.1.113719.1.450.4.105 NAME
'srvprvLocalizedDescrs' DESC 'Provides set of localized description
strings for the provisioning web applications, Designers and
iManager.' SYNTAX  1.3.6.1.4.1.1466.115.121.1.26 ) dn: cn=schema
changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.106 NAME 'srvprvStatus' DESC 'Specifies the
status of the Provisioning Object. Supported values will include:
Inactive, Active, Template, and Retired.' SYNTAX
1.3.6.1.4.1.1466.115.121.1.26 SINGLE-VALUE ) dn: cn=schema changetype:
modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.107 NAME 'srvprvProcessXML' DESC 'XML
document representing a Provisioning process definition including
Workflow and Provisioning Action.' SYNTAX
1.3.6.1.4.1.1466.115.121.1.5 SINGLE-VALUE ) dn: cn=schema changetype:
modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.108 NAME 'srvprvEntityType' DESC 'Specifies
Directory Abstraction Layer Entity definition type: P-Public
definitions or S-System definitions.' SYNTAX
1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE ) dn: cn=schema changetype:
modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.109 NAME 'srvprvRequestXML' DESC 'XML
document representing the initial request form and its data bindings'
SYNTAX  1.3.6.1.4.1.1466.115.121.1.5 SINGLE-VALUE ) dn: cn=schema
changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.110 NAME 'srvprvModified' DESC 'Flag to
indicate changes to definitions object instances in the directory
model container' SYNTAX  1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
dn: cn=schema changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.111 NAME 'srvprvEntitlementRef' DESC
'Reference to a DirXML-Entitlement' SYNTAX
1.3.6.1.4.1.1466.115.121.1.12 SINGLE-VALUE ) #-----------------------
```

```
----------------------------------------------------------------------
------------------------------ #-- Provisioning Configuration
Containers #----------------------------------------------------------
------------------------------------------------------------------ dn:
cn=schema changetype: modify add: objectclasses objectClasses: (
2.16.840.1.113719.1.450.6.100 NAME 'srvprvAppConfig' DESC 'Container
for application configuration objects of the Provisioning System to
which its DirXML-Driver parent connects.' SUP top STRUCTURAL MUST ( cn
$ version ) MAY ( description ) X-NDS_NAMING ( 'cn' ) X-NDS_CONTAINMENT
( 'DirXML-Driver' ) ) dn: cn=schema changetype: modify add:
objectclasses objectClasses: ( 2.16.840.1.113719.1.450.6.101 NAME
'srvprvRequestDefs' DESC 'Container for Provisioning Request
Definitions, the set of provisionable items to the Web Application run-
time.' SUP top STRUCTURAL MUST ( cn ) MAY ( description ) X-NDS_NAMING
( 'cn' ) X-NDS_CONTAINMENT ( 'srvprvAppConfig' ) ) dn: cn=schema
changetype: modify add: objectclasses objectClasses: (
2.16.840.1.113719.1.450.6.102 NAME 'srvprvWorkflowDefs' DESC
'Container for Workflow objects, including design-time descriptions
plus any template or unused flows.' SUP top STRUCTURAL MUST ( cn ) MAY
( description ) X-NDS_NAMING ( 'cn' ) X-NDS_CONTAINMENT (
'srvprvAppConfig' ) ) dn: cn=schema changetype: modify add:
objectclasses objectClasses: ( 2.16.840.1.113719.1.450.6.103 NAME
'srvprvWorkflowDefs' DESC 'Container for Workflow objects, including
design-time descriptions plus any template or unused flows.' SUP top
STRUCTURAL MUST ( cn ) MAY ( description ) X-NDS_NAMING ( 'cn' ) X-
NDS_CONTAINMENT ( 'srvprvAppConfig' ) ) dn: cn=schema changetype:
modify add: objectclasses objectClasses: (
2.16.840.1.113719.1.450.6.104 NAME 'srvprvServiceDefs' DESC 'Container
for Service Definition objects, which wrap Web Services called by
Workflows.' SUP top STRUCTURAL MUST ( cn ) MAY ( description ) X-
NDS_NAMING ( 'cn' ) X-NDS_CONTAINMENT ( 'srvprvAppConfig' ) ) dn:
cn=schema changetype: modify add: objectclasses objectClasses: (
2.16.840.1.113719.1.450.6.105 NAME 'srvprvDirectoryModel' DESC
'Container for Directory Abstraction Layer meta-level objects,
selected contents of the directory to be exposed by the Identity
Portlets and Web Applications.' SUP top STRUCTURAL MUST ( cn ) MAY (
description $ srvprvModified ) X-NDS_NAMING ( 'cn' ) X-NDS_CONTAINMENT
( 'srvprvAppConfig' ) ) dn: cn=schema changetype: modify add:
objectclasses objectClasses: ( 2.16.840.1.113719.1.450.6.106 NAME
'srvprvAppDefs' DESC 'Container for configuration objects used to
initialise the Provisioning run-time environment, such as themes for
the Identity Portal.' SUP top STRUCTURAL MUST ( cn ) MAY ( description
) X-NDS_NAMING ( 'cn' ) X-NDS_CONTAINMENT ( 'srvprvAppConfig' ) ) dn:
cn=schema changetype: modify add: objectclasses objectClasses: (
2.16.840.1.113719.1.450.6.111 NAME 'srvprvEntityDefs' DESC 'Container
for Directory Abstraction Layer Entity defintions, to be exposed by the
Identity Portlets and Web Applications.' SUP top STRUCTURAL MUST ( cn )
MAY ( description ) X-NDS_NAMING ( 'cn' ) X-NDS_CONTAINMENT (
'srvprvDirectoryModel' ) ) dn: cn=schema changetype: modify add:
objectclasses objectClasses: ( 2.16.840.1.113719.1.450.6.112 NAME
'srvprvRelationshipDefs' DESC 'Container for Directory Abstraction
Layer Relationship definitions, to be exposed by the Identity Portlets
and Web Applications.' SUP top STRUCTURAL MUST ( cn ) MAY ( description
) X-NDS_NAMING ( 'cn' ) X-NDS_CONTAINMENT ( 'srvprvDirectoryModel' ) )
```

```
dn: cn=schema changetype: modify add: objectclasses objectClasses: (
2.16.840.1.113719.1.450.6.113 NAME 'srvprvChoiceDefs' DESC 'Container
for Directory Abstraction Layer Choice definitions, to be exposed by
the Identity Portlets and Web Applications.' SUP top STRUCTURAL MUST (
cn ) MAY ( description ) X-NDS_NAMING ( 'cn' ) X-NDS_CONTAINMENT (
'srvprvDirectoryModel' ) ) #### Provisioning Configuration Object
Classes dn: cn=schema changetype: modify add: objectclasses
objectClasses: ( 2.16.840.1.113719.1.450.6.107 NAME 'srvprvRequest'
DESC 'Exposes one provisionable item to be granted or revoked,
including the workflow process which defines the run-time aspects of
the Workflow and Provisioning Target.' SUP top STRUCTURAL MUST ( cn $
srvprvStatus $ srvprvFlowStrategy $ srvprvGrant $ srvprvRevoke $
srvprvCategoryKey $ srvprvLocalizedNames $ srvprvLocalizedDescrs ) MAY
( description $ srvprvEntitlementRef $ XmlData $ srvprvRequestXML $
srvprvProcessXML ) X-NDS_NOT_CONTAINER '1' X-NDS_NAMING ( 'cn' ) X-
NDS_CONTAINMENT ( 'srvprvRequestDefs' ) ) dn: cn=schema changetype:
modify add: objectclasses objectClasses: (
2.16.840.1.113719.1.450.6.108 NAME 'srvprvWorkflow' DESC 'Defines the
network of activites including traversal conditions to be executed in
order to obtain approval for a provisioning action.' SUP top STRUCTURAL
MUST ( cn $ srvprvLocalizedNames $ srvprvLocalizedDescrs  ) MAY (
description $ XmlData ) X-NDS_NOT_CONTAINER '1' X-NDS_NAMING ( 'cn' )
X-NDS_CONTAINMENT ( 'srvprvWorkflowDefs' ) ) dn: cn=schema changetype:
modify add: objectclasses objectClasses: (
2.16.840.1.113719.1.450.6.109 NAME 'srvprvResource' DESC 'Defines the
set of directory assignments to execute for a provisioning fulfillment
operation (either Grant or Revoke).' SUP top STRUCTURAL MUST ( cn $
srvprvLocalizedNames $ srvprvLocalizedDescrs ) MAY ( description $
srvprvEntitlementRef $ XmlData ) X-NDS_NOT_CONTAINER '1' X-NDS_NAMING
( 'cn' ) X-NDS_CONTAINMENT ( 'srvprvResourceDefs' ) ) dn: cn=schema
changetype: modify add: objectclasses objectClasses: (
2.16.840.1.113719.1.450.6.110 NAME 'srvprvService' DESC 'Describes how
to invoke a specific Web Service from an Workflow. This includes
specification of input and return values.' SUP top STRUCTURAL MUST ( cn
) MAY ( description $ XmlData ) X-NDS_NOT_CONTAINER '1' X-NDS_NAMING (
'cn' ) X-NDS_CONTAINMENT ( 'srvprvServiceDefs' ) ) dn: cn=schema
changetype: modify add: objectclasses objectClasses: (
2.16.840.1.113719.1.450.6.109 NAME 'srvprvResource' DESC 'Defines the
set of directory assignments to execute for a provisioning fulfillment
operation (either Grant or Revoke).' SUP top STRUCTURAL MUST ( cn $
srvprvLocalizedNames $ srvprvLocalizedDescrs ) MAY ( description $
srvprvEntitlementRef $ XmlData ) X-NDS_NOT_CONTAINER '1' X-NDS_NAMING
( 'cn' ) X-NDS_CONTAINMENT ( 'srvprvResourceDefs' ) ) dn: cn=schema
changetype: modify add: objectclasses objectClasses: (
2.16.840.1.113719.1.450.6.115 NAME 'srvprvRelationship' DESC 'Defines
relationships between objects in the directory, for use in the Identity
Portlets and other Web Application components.' SUP top STRUCTURAL
MUST ( cn ) MAY ( description $ XmlData ) X-NDS_NOT_CONTAINER '1' X-
NDS_NAMING ( 'cn' ) X-NDS_CONTAINMENT ( 'srvprvRelationshipDefs' ) )
dn: cn=schema changetype: modify add: objectclasses objectClasses: (
2.16.840.1.113719.1.450.6.116 NAME 'srvprvChoice' DESC 'Enumeration of
values which can be assigned to a particular attribute, used in a
query, etc. for use in the Identity Portlets and other Web Application
components.' SUP top STRUCTURAL MUST ( cn ) MAY ( description $ XmlData
```

```
) X-NDS_NOT_CONTAINER '1' X-NDS_NAMING ( 'cn' ) X-NDS_CONTAINMENT (
'srvprvChoiceDefs' ) ) dn: cn=schema changetype: modify add:
objectclasses objectClasses: ( 2.16.840.113719.1.450.6.117 NAME
'srvprvDirectoryModelConfig' DESC 'Runtime Directory Abstraction Layer
configurarion parameters' SUP top STRUCTURAL MUST ( cn ) MAY (
description $ XmlData ) X-NDS_NOT_CONTAINER '1' X-NDS_NAMING ( 'cn' )
X-NDS_CONTAINMENT ( 'srvprvDirectoryModel' ) ) #### User Aux Classes
and Attributes dn: cn=schema changetype: modify add: attributeTypes
attributeTypes: ( 2.16.840.1.113719.1.450.4.80 NAME 'srvprvAssetRef'
DESC 'Representation of the aggregate asset properties for a named
asset associated to a user via the srvprvAssetRecipientAux class.'
SYNTAX 2.16.840.1.113719.1.1.5.1.6 ) dn: cn=schema changetype: modify
add: objectclasses objectClasses: ( 2.16.840.1.113719.1.450.6.80 NAME
'srvprvAssetRecipientAux' DESC 'Records the provisioning of non-IT
assets on a user' AUXILIARY MAY ( srvprvAssetRef ) ) #----------------
----------------------------------------------------------------------
-------------------------------------- #-- Web Application Config
Class #---------------------------------------------------------------
------------------------------------------------------------- dn:
cn=schema changetype: modify add: attributeTypes attributeTypes:
(2.16.840.1.113719.1.450.4.20 NAME 'srvprvDefaultTheme' DESC 'The
default theme' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE ) dn:
cn=schema changetype: modify add: objectclasses objectClasses: (
2.16.840.1.113719.1.450.6.21 NAME 'srvprvWebAppConfig' DESC 'Web
Application Config Object' SUP top STRUCTURAL MUST (cn) MAY
(description $ srvprvDefaultTheme $ XmlData ) X-NDS_NOT_CONTAINER '1'
X-NDS_NAMING 'cn' X-NDS_CONTAINMENT ( 'srvprvAppDefs' ) ) #-----------
------------------------------------------------------- -------------
------------------------------------------- #-- Theme Branding
Structural Class #----------------------------------------------------
----------------------------------------------------------------------
-- dn: cn=schema changetype: modify add: attributeTypes
attributeTypes: ( 2.16.840.1.113719.1.450.4.21 NAME
'srvprvHeaderLogoImage' DESC 'Header Logo Primary Image' SYNTAX
1.3.6.1.4.1.1466.115.121.1.5 SINGLE-VALUE ) dn: cn=schema changetype:
modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.22 NAME 'srvprvHeaderLogoFile' DESC 'Header
Logo Primary Image File Name' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE ) dn: cn=schema changetype: modify add: attributeTypes
attributeTypes: ( 2.16.840.1.113719.1.450.4.23 NAME
'srvprvHeaderLogoLastMod' DESC 'Header Logo Primary Last Modified'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE ) dn: cn=schema
changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.24 NAME 'srvprvHeaderLogo2Image' DESC
'Header Logo Secondary Image' SYNTAX 1.3.6.1.4.1.1466.115.121.1.5
SINGLE-VALUE ) dn: cn=schema changetype: modify add: attributeTypes
attributeTypes: ( 2.16.840.1.113719.1.450.4.25 NAME
'srvprvHeaderLogo2File' DESC 'Header Logo Secondary Image File Name'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 | SINGLE-VALUE ) dn: cn=schema
changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.26 NAME 'srvprvHeaderLogo2LastMod' DESC
'Header Logo Secondary Last Modified' SYNTAX
1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE ) dn: cn=schema changetype:
modify add: attributeTypes attributeTypes: (
```

```
2.16.840.1.113719.1.450.4.27 NAME 'srvprvHeaderTextureImage' DESC
'Header Texture Image' SYNTAX 1.3.6.1.4.1.1466.115.121.1.5 SINGLE-
VALUE ) dn: cn=schema changetype: modify add: attributeTypes
attributeTypes: ( 2.16.840.1.113719.1.450.4.28 NAME
'srvprvHeaderTextureFile' DESC 'Header Texture File Name' SYNTAX
1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE ) dn: cn=schema changetype:
modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.29 NAME 'srvprvHeaderTextureLastMod' DESC
'Header Texture Last Modified' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE ) dn: cn=schema changetype: modify add: attributeTypes
attributeTypes: ( 2.16.840.1.113719.1.450.4.30 NAME
'srvprvHeaderFillerImage' DESC 'Header Filler Image' SYNTAX
1.3.6.1.4.1.1466.115.121.1.5 SINGLE-VALUE ) dn: cn=schema changetype:
modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.31 NAME 'srvprvHeaderFillerFile' DESC
'Header Filler File Name' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-
VALUE ) dn: cn=schema changetype: modify add: attributeTypes
attributeTypes: ( 2.16.840.1.113719.1.450.4.32 NAME
'srvprvHeaderFillerLastMod' DESC 'Header Filler Last Modified' SYNTAX
1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE ) dn: cn=schema changetype:
modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.33 NAME 'srvprvLoginImage' DESC 'Login
Image' SYNTAX 1.3.6.1.4.1.1466.115.121.1.5 SINGLE-VALUE ) dn:
cn=schema changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.34 NAME 'srvprvLoginFile' DESC 'Login File
Name' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE ) dn:
cn=schema changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.35 NAME 'srvprvLoginLastMod' DESC 'Login
Last Modified' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE ) dn:
cn=schema changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.36 NAME 'srvprvLoginSmallImage' DESC 'Login
Small Image' SYNTAX 1.3.6.1.4.1.1466.115.121.1.5 SINGLE-VALUE ) dn:
cn=schema changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.37 NAME 'srvprvLoginSmallFile' DESC 'Login
Small File Name' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
dn: cn=schema changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.38 NAME 'srvprvLoginSmallLastMod' DESC
'Login Small Last Modified' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE ) dn: cn=schema changetype: modify add: attributeTypes
attributeTypes: ( 2.16.840.1.113719.1.450.4.39 NAME 'srvprvNavColor'
DESC 'Navigation Color' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-
VALUE ) dn: cn=schema changetype: modify add: attributeTypes
attributeTypes: ( 2.16.840.1.113719.1.450.4.40 NAME
'srvprvNavColorLastMod' DESC 'Navigation Color Last Modified' SYNTAX
1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE ) dn: cn=schema changetype:
modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.41 NAME 'srvprvNavBckgrColor' DESC
'Navigation Background Color' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE ) dn: cn=schema changetype: modify add: attributeTypes
attributeTypes: ( 2.16.840.1.113719.1.450.4.42 NAME
'srvprvNavBckgrColorLastMod' DESC 'Navigation Background Color Last
Modified' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE ) dn:
cn=schema changetype: modify add: objectclasses objectClasses: (
2.16.840.1.113719.1.450.6.20 NAME 'srvprvTheme' DESC 'Theme Object'
```

```
SUP top STRUCTURAL MUST (cn) MAY (description $ srvprvHeaderLogoImage
$ srvprvHeaderLogoFile $ srvprvHeaderLogoLastMod $
srvprvHeaderLogo2Image $ srvprvHeaderLogo2File $
srvprvHeaderLogo2LastMod $ srvprvHeaderTextureImage $
srvprvHeaderTextureFile $ srvprvHeaderTextureLastMod $
srvprvHeaderFillerImage $ srvprvHeaderFillerFile $
srvprvHeaderFillerLastMod $ srvprvLoginImage $ srvprvLoginFile $
srvprvLoginLastMod $ srvprvLoginSmallImage $ srvprvLoginSmallFile $
srvprvLoginSmallLastMod $ srvprvNavColor $ srvprvNavColorLastMod $
srvprvNavBckgrColor $ srvprvNavBckgrColorLastMod ) X-NDS_NOT_CONTAINER
'1' X-NDS_CONTAINMENT ( 'srvprvAppDefs' ) X-NDS_NAMING 'cn' ) #-------
----------------------------------------------------------------------
----------------------------------------------- #-- Attributes,
objects, and containers for Proxy, Delegatee and User availability, #-
----------------------------------------------------------------------
----------------------------------------------------- dn: cn=schema
changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.120 NAME 'srvprvAssignFromUser' DESC 'User
subjects of a proxy or delegatee assignment' SYNTAX
1.3.6.1.4.1.1466.115.121.1.12 ) dn: cn=schema changetype: modify add:
attributeTypes attributeTypes: ( 2.16.840.1.113719.1.450.4.121 NAME
'srvprvAssignFromGroup' DESC 'Group subjects of a proxy or delegatee
assignment' SYNTAX  1.3.6.1.4.1.1466.115.121.1.12 ) dn: cn=schema
changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.122 NAME 'srvprvAssignFromContainer' DESC
'Container subjects of a proxy or delegatee assignment' SYNTAX
1.3.6.1.4.1.1466.115.121.1.12 ) dn: cn=schema changetype: modify add:
attributeTypes attributeTypes: ( 2.16.840.1.113719.1.450.4.123 NAME
'srvprvAssignToUser' DESC 'The User targets of a proxy or delegatee
assignment' SYNTAX  1.3.6.1.4.1.1466.115.121.1.12 ) dn: cn=schema
changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.124 NAME 'srvprvAssignToRelationship' DESC
'A target relationship of a delegatee assignment' SYNTAX
1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE ) dn: cn=schema changetype:
modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.125 NAME 'srvprvAssignExpiration' DESC 'Time
at which a proxy or delegatee assignment expires' SYNTAX
1.3.6.1.4.1.1466.115.121.1.24 SINGLE-VALUE ) dn: cn=schema changetype:
modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.126 NAME 'srvprvRequestDefName' DESC 'The
provisioning request definition name associated with a delegatee
definition.' SYNTAX  1.3.6.1.4.1.1466.115.121.1.12 ) dn: cn=schema
changetype: modify add: objectclasses objectClasses: (
2.16.840.1.113719.1.450.6.120 NAME 'srvprvProxyDefs' DESC 'Container
for proxy definitions.' SUP top STRUCTURAL MUST ( cn ) MAY (
description ) X-NDS_NAMING ( 'cn' ) X-NDS_CONTAINMENT (
'srvprvAppConfig' ) ) dn: cn=schema changetype: modify add:
objectclasses objectClasses: ( 2.16.840.1.113719.1.450.6.121 NAME
'srvprvDelegateeDefs' DESC 'Container for delegatee definitions.' SUP
top STRUCTURAL MUST ( cn ) MAY ( description ) X-NDS_NAMING ( 'cn' ) X-
NDS_CONTAINMENT ( 'srvprvAppConfig' ) ) dn: cn=schema changetype:
modify add: objectclasses objectClasses: (
2.16.840.1.113719.1.450.6.122 NAME 'srvprvProxyAssignment' DESC 'Proxy
assignment definition' SUP top STRUCTURAL MUST ( cn $
```

```
srvprvAssignToUser ) MAY ( description $ srvprvAssignFromUser $
srvprvAssignFromGroup $ srvprvAssignFromContainer $
srvprvAssignExpiration ) X-NDS_NAMING ( 'cn' ) X-NDS_CONTAINMENT (
'srvprvProxyDefs' ) ) dn: cn=schema changetype: modify add:
objectclasses objectClasses: ( 2.16.840.1.113719.1.450.6.123 NAME
'srvprvDelegateeAssignment' DESC 'Delegatee assignment definition' SUP
top STRUCTURAL MUST cn MAY ( srvprvRequestDefName $ description $
srvprvAssignFromUser $ srvprvAssignFromGroup $
srvprvAssignFromContainer $ srvprvAssignToUser $
srvprvAssignToRelationship $ srvprvAssignExpiration ) X-NDS_NAMING (
'cn' ) X-NDS_CONTAINMENT ( 'srvprvDelegateeDefs' ) ) ############## DO
NOT DELETE THIS LINE ##################
#########################################################
```

Configurando o Arquivo de Aplicativo

B

Este apêndice descreve as configurações avançadas que podem ser definidas apenas com a edição do arquivo WAR do aplicativo de usuário. Os tópicos incluem:

B.1 Sobre o WAR do aplicativo de usuário

O aplicativo de usuário do Identity Manager é fornecido em um pacote como um arquivo de aplicativo Web (WAR - Web Application Archive) compatível com J2EE. O arquivo WAR do aplicativo de usuário contém um conjunto de classes Java e arquivos XML que controlam o comportamento do aplicativo em tempo de execução. Em geral, o WAR não deve ser modificado. Entretanto, em algumas raras situações, pode ser necessário abrir o arquivo WAR e efetuar pequenas mudanças para controlar o comportamento do aplicativo.

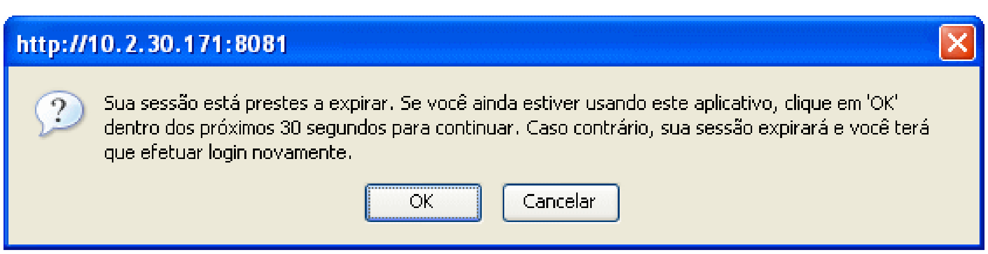
Observação: O restante deste apêndice supõe que você esteja familiarizado com conceitos e procedimentos do J2EE. Caso não tenha certeza sobre como efetuar mudanças em um arquivo WAR, consulte a documentação do J2EE.

B.2 Definindo o tempo de espera da sessão

Para evitar que o servidor fique sobrecarregado com sessões inativas, o aplicativo de usuário do Identity Manager coloca em tempo de espera a sessão do usuário que permanece inativa por um longo período. O intervalo de tempo de espera padrão é de 10 minutos. Para mudar o padrão, edite o arquivo *web.xml* na pasta WEB-INF do arquivo WAR do aplicativo de usuário.

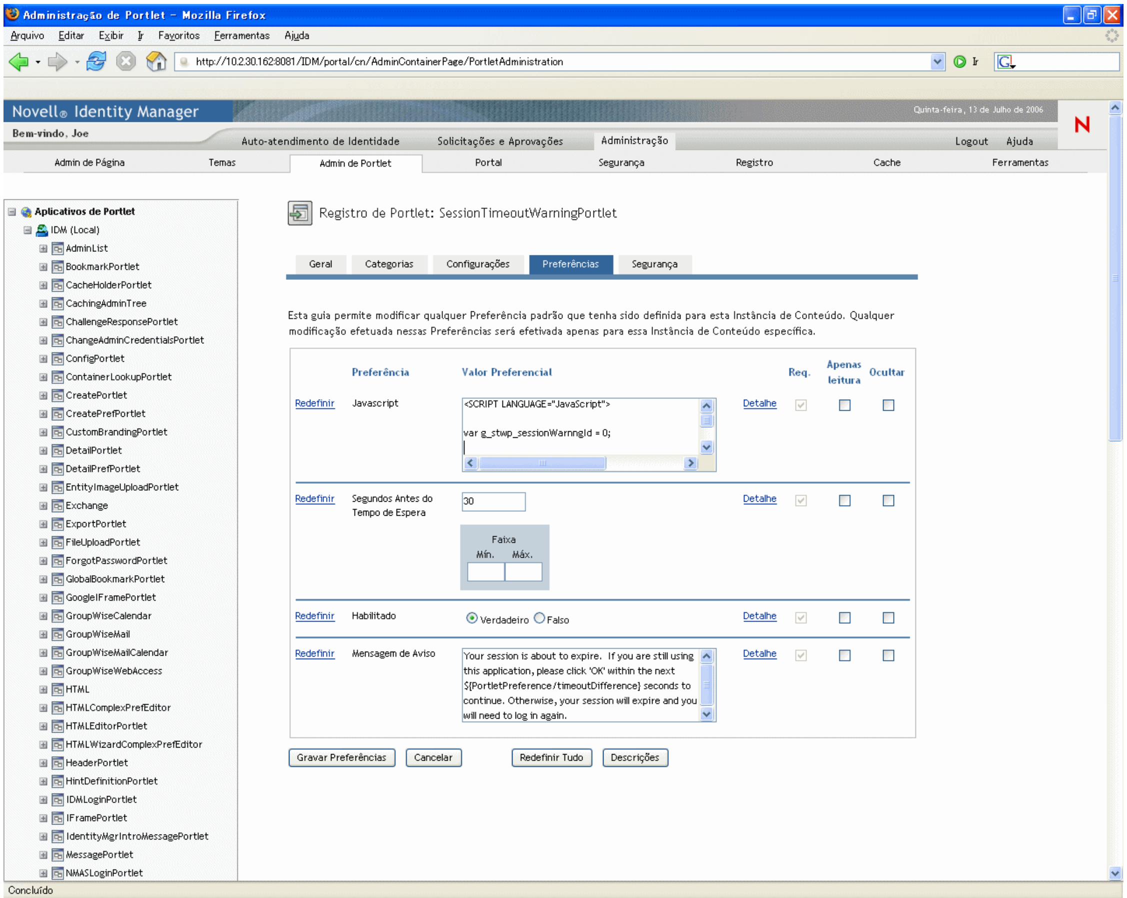
Editando o intervalo de tempo de espera da sessão O arquivo web.xml no WAR tem um elemento chamado <*session-timeout*> (que pode ser encontrado no elemento <*session-config*>) que especifica quanto tempo uma sessão pode permanecer inativa antes de entrar em tempo de espera. Para definir o intervalo de tempo de espera da sessão, mude o valor desse elemento. O valor deve ser especificado em minutos.

Controlando o comportamento da mensagem de alerta Por padrão, o aplicativo de usuário do Identity Manager exibe uma mensagem de alerta sempre que uma sessão do usuário está para entrar em tempo de espera.



Se o usuário não responder à mensagem ao clicar em OK, ocorrerá tempo de espera da sessão. A mensagem de alerta é habilitada por padrão. Se quiser, você pode desabilitá-la. Você também pode especificar quanto tempo o usuário pode levar até responder à mensagem de alerta.

Para controlar o comportamento da mensagem de alerta, é preciso configurar *SessionTimeoutWarningPortlet*. Para isso, é preciso editar as preferências do portlet no registro do portlet, como indicado abaixo:



Para especificar quanto tempo o usuário terá até responder à mensagem de alerta, edite o valor de *Segundos Antes do Tempo de Espera*. Para desabilitar a mensagem de alerta, clique em *Falso* ao lado de *Habilitado*. Quando você terminar de efetuar mudanças, clique em *Gravar Preferências*.